Calhoun
Institutional Archive of the Naval Postgraduate School

**Calhoun: The NPS Institutional Archive**

**DSpace Repository**

Theses and Dissertations | 1. Thesis and Dissertation Collection, all items

2005-03

# A case study of Internet Protocol Telephony implementation at United States Coast Guard headquarters

Patton, Mark B.

Monterey  California. Naval Postgraduate School

http://hdl.handle.net/10945/2221

This publication is a work of the U.S. Government as defined in Title 17, United States Code, Section 101. Copyright protection is not available for this work in the United States.

*Downloaded from NPS Archive: Calhoun*

DUDLEY KNOX LIBRARY

Calhoun is the Naval Postgraduate School's public access digital repository for research materials and institutional publications created by the NPS community. Calhoun is named for Professor of Mathematics Guy K. Calhoun, NPS's first appointed -- and published -- scholarly author.

Dudley Knox Library / Naval Postgraduate School
411 Dyer Road / 1 University Circle
Monterey, California USA 93943

http://www.nps.edu/library

# NAVAL POSTGRADUATE SCHOOL

**MONTEREY, CALIFORNIA**

# THESIS

**A CASE STUDY OF INTERNET PROTOCOL TELEPHONY (IPT) IMPLEMENTATION AT UNITED STATES COAST GUARD HEADQUARTERS**

by

Mark B. Patton

March 2005

Co-Advisors: Dan C. Boger
R. Scott Coté

**Approved for public release, distribution is unlimited.**

THIS PAGE INTENTIONALLY LEFT BLANK

| REPORT DOCUMENTATION PAGE | *Form Approved OMB No. 0704-0188* |
|---|---|

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.

| **1. AGENCY USE ONLY *(Leave blank)*** | **2. REPORT DATE** March 2005 | **3. REPORT TYPE AND DATES COVERED** Master's Thesis |
|---|---|---|

**4. TITLE AND SUBTITLE**: A Case Study of Internet Protocol Telephony (IPT) Implementation at United States Coast Guard Headquarters

**5. FUNDING NUMBERS**

**6. AUTHOR(S)** Mark Patton

**7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)**
Naval Postgraduate School
Monterey, CA 93943-5000

**8. PERFORMING ORGANIZATION REPORT NUMBER**

**9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES)**
USCG Headquarters Support Command
2100 Second Street SW
Washington D.C. 20593-0001

**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**

**11. SUPPLEMENTARY NOTES** The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

**12a. DISTRIBUTION / AVAILABILITY STATEMENT**
Approved for public release; distribution is unlimited.

**12b. DISTRIBUTION CODE**

**13. ABSTRACT (maximum 200 words)**

Recent advances in information technology communications have brought about increases in bandwidth and processing speeds to encourage the growth of Internet Protocol Telephony (IPT), a method of transmitting voice conversations over data networks. Many organizations are replacing portions of their traditional phone systems to gain the benefits of cost savings and enhanced feature sets through the use of IPT. The Coast Guard has an interest in exploiting this technology, and has taken its first steps by implementing IPT at Headquarters Support Command in Washington D.C. This thesis investigates the successful implementation practices and security policies of commercial, educational, and government organizations in order to create recommendations for IPT security policies and implementation practices relevant to the Coast Guard. It includes the discussion of the public switched telephone network, an overview of IPT, IPT security issues, the safeguards available to counter security threats, the tradeoffs (e.g., voice quality, cost) required to mitigate security risks, and current IPT security policy and implementation guidance. It is supported by the study and analysis of the IPT system at Coast Guard Headquarters. The Coast Guard gains an understanding of the advantages, limitations, and security issues that it will face as it considers further implementation of IPT.

**14. SUBJECT TERMS** Voice Over Internet Protocol, VOIP, Internet Protocol Telephony, IP Telephony, Security, Policy, Implementation Guide, Coast Guard

**15. NUMBER OF PAGES** 205

**16. PRICE CODE**

| **17. SECURITY CLASSIFICATION OF REPORT** | **18. SECURITY CLASSIFICATION OF THIS PAGE** | **19. SECURITY CLASSIFICATION OF ABSTRACT** | **20. LIMITATION OF ABSTRACT** |
|---|---|---|---|
| Unclassified | Unclassified | Unclassified | UL |

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

**Approved for public release, distribution is unlimited.**

# A CASE STUDY OF INTERNET PROTOCOL TELEPHONY IMPLEMENTATION AT UNITED STATES COAST GUARD HEADQUARTERS

Mark B. Patton
Lieutenant, United States Coast Guard
B.S., United States Coast Guard Academy, 1999

Submitted in partial fulfillment of the
requirements for the degree of

**MASTER OF SCIENCE IN INFORMATION TECHNOLOGY MANAGEMENT**

from the

**NAVAL POSTGRADUATE SCHOOL**
**March 2005**

Author: Mark B. Patton

Approved by: Dan C. Boger
Co-Advisor

R. Scott Coté
Co-Advisor

Dan C. Boger
Chairman, Information Sciences Department

THIS PAGE INTENTIONALLY LEFT BLANK

# ABSTRACT

Recent advances in information technology communications have brought about increases in bandwidth and processing speeds to encourage the growth of Internet Protocol Telephony (IPT), a method of transmitting voice conversations over data networks. Many organizations are replacing portions of their traditional phone systems to gain the benefits of cost savings and enhanced feature sets through the use of IPT. The Coast Guard has an interest in exploiting this technology, and has taken its first steps by implementing IPT at Headquarters Support Command in Washington, D.C. This thesis investigates the successful implementation practices and security policies of commercial, educational, and government organizations in order to create recommendations for IPT security policies and implementation practices relevant to the Coast Guard. It includes the discussion of the public switched telephone network, an overview of IPT, IPT security issues, the safeguards available to counter security threats, the tradeoffs (e.g., voice quality, cost) required to mitigate security risks, and current IPT security policy and implementation guidance. It is supported by the study and analysis of the IPT system at Coast Guard Headquarters. The Coast Guard gains an understanding of the advantages, limitations, and security issues that it will face as it considers further implementation of IPT.

THIS PAGE INTENTIONALLY LEFT BLANK

## TABLE OF CONTENTS

# LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

## LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

## LIST OF ACRONYMS AND ABBREVIATIONS

| | |
|---|---|
| AH | Authentication Header |
| ALG | Application Layer Gateway |
| ARP | Address Resolution Protocol |
| C4&IT | Command, Control, Communications, Computers, and Information Technology |
| CALEA | Communications for Law Enforcement Act of 1994 |
| CDR | Call Detail Records |
| CG | Coast Guard |
| CGAP | Coast Guard Acquisition Procedures |
| CGHQ | Coast Guard Headquarters |
| CIS | Classified Information Systems |
| CM | Configuration Management |
| Codec | Coder/Decoder, Compressor/Decompressor |
| cRTP | RTP header compression |
| CWPS | Connected Work Place Solutions |
| DAA | Designated Accrediting Authorities |
| DDoS | Distributed Denial of Service |
| DHS | Department of Homeland Security |
| DISA | Defense Information Systems Agency |
| DoD | Department of Defense |
| DoS | Denial of Service |
| DoT | Department of Transportation |
| DS0 | Digital Signal Level 0 |
| E911 | Emergency 911 |
| ESP | Encapsulating Security Payload |
| ETSI | European Telecommunications Standards Institute |
| FCP | Firewall Control Proxy |

| | |
|---|---|
| FIPS | Federal Information Processing Standard |
| GETS | Government Telecommunications Service |
| HIDS | Host-based Intrusion Detection System |
| HQ | Headquarters |
| HSC | Headquarters Support Command |
| HVAC | Heating, Ventilation, and Air Conditioning |
| IA | Information Assurance |
| IAM | Information Assurance Manual |
| ICE | Interactive Connectivity Establishment |
| IDS | Intrusion Detection System |
| IETF | Internet Engineering Task Force |
| IP | Internet Protocol |
| IPsec | Internet Protocol Security |
| IPT | Internet Protocol Telephony |
| ISP | Internet Service Provider |
| IT | Information Technology |
| ITU | International Telecommunication Union |
| LAN | Local Area Network |
| MAC | Moves, Adds, Changes |
| Mbps | Megabits per second |
| MCU | Multipoint Control Unit |
| MEGACO | Media Gateway Control |
| MG | Media Gateway |
| MGC | Media Gateway Controller |
| MGCP | Media Gateway Control Protocol |
| MOS | Mean Opinion Score |
| NAT | Network Address Translation |
| NIDS | Network Intrusion Detection System |
| NIS | Non-critical Information System |
| NIST | National Institute of Standards and Technology |

| | |
|---|---|
| PBX | Private Branch Exchange |
| PC | Personal Computer |
| PED | Personal Electronic Device |
| POTS | Plain Old Telephone System |
| PS&FPP | Physical Security and Force Protection Program |
| PSTN | Public Switched Telephone Network |
| QoS | Quality of Service |
| RAID | Redundant Array of Independent Disks |
| RAS | Registration, Admissions, and Status or Remote Access Server |
| RFC | Request For Comment |
| RSVP | Reservation Protocol |
| RTP | Real-Time Transport Protocol |
| SCIS | Sensitive/Critical Information System |
| SCP | Service Control Point |
| SDLC | Systems Development Life Cycle |
| SG | Signaling Gateway |
| SIP | Session Initiation Protocol |
| SLA | Service Level Agreement |
| SRTP | Secure Real-time Transport Protocol |
| SS7 | Signaling System 7 |
| SSH | Secure Shell |
| SSP | Service Switching Point |
| STP | Signal Transfer Point |
| STUN | Simple Traversal of UDP through NAT |
| T1 | Trunk Level 1 |
| TCP | Transmission Control Protocol |
| TFTP | Trivial File Transfer Protocol |
| TISCOM | Telecommunications Command |
| TLS | Transport Level Security |

| | |
|---|---|
| TURN | Traversal Using Relay NAT |
| UA | User Agent |
| UAC | User Agent Client |
| UAS | User Agent Server |
| UDP | User Datagram Protocol |
| UMS | Unified Messaging System |
| URL | Uniform Resource Locator |
| VAD | Voice Activity Detection |
| VLAN | Virtual Local Area Network |
| VoIP | Voice over Internet Protocol |
| VON | Voice on the Net |
| VPN | Virtual Private Network |
| WAN | Wide Area Network |
| WEP | Wired Equivalent Privacy |
| WPA | WiFi Protected Access |

# ACKNOWLEDGMENTS

I would like to thank all of those who provided guidance, assistance, and support through the Thesis process.

I value the support received and learning experiences shared with a variety of staff and students at NPS. I appreciate the assistance of my thesis advisors, Professor Dan Boger and Scott Coté, who provided direction and feedback throughout the process. I recognize the effort required by the Thesis Processing Office to handle the difficult responsibility of ensuring that quality documents leave this school. I'm also grateful for the effort of Jean Brennan who goes out of her way every day to serve the ITM and CS students.

I would like to thank all of the Coast Guard and Civilian personnel who assisted me at Coast Guard Headquarters Support Command. I'm particularly grateful for the efforts of CDR Kip Whiteman who located funding; mentored, encouraged, and guided me through the initial stages of the thesis development; and supported my efforts throughout. Thanks also go to Tom Estes who took the time to share his knowledge and expertise. I also appreciate the assistance provided by CWO Perry Darley, Audrey Alleyne, Joe Krejci, and Jim McCool (CWPS).

Finally, I would like to acknowledge my wife, Holly, for her constant love and support in all my pursuits, and especially through the trials of this thesis. I'm eternally

grateful for her faith in me and her devotion to my happiness.

THIS PAGE INTENTIONALLY LEFT BLANK

# I. INTRODUCTION

## A. BACKGROUND

Recent advances in information technology communications have brought about increases in bandwidth and processing speeds to encourage the growth of Internet Protocol Telephony (IPT), a method of transmitting voice conversations over data networks. Many organizations are replacing portions of their traditional phone systems to gain the benefits of cost savings and enhanced feature sets through the use of IPT.

The Coast Guard (CG) has an interest in exploiting this technology, and has taken its first steps by implementing IPT at Headquarters Support Command in Washington, D.C. Unfortunately, the Coast Guard has little to no policy in place to guide the employment of a high quality, secure, and reliable IPT-based network. To address this issue, this thesis research will: (1) explore the successful implementation practices and security policies of commercial, government, and educational organizations, (2) produce recommendations for IPT security policies and IPT implementation practices relevant to the Coast Guard, and (3) analyze the IPT system at CG Headquarters with respect to those policy recommendations.

## B. ORGANIZATION

Following this introduction, Chapter II will explain the basic characteristics and operation of the Public Switched Telephone Network (PSTN) and Internet Protocol Telephony (IPT). It will facilitate a comparison between the two types of telephone networks and prepare the reader to understand discussions about IPT security and

implementation. Chapter III will provide an analysis of IPT security issues specifically addressing IPT specific threats, vulnerabilities, and safeguards. It will also include a discussion of policies and guidance that address IPT security. Chapter IV will present an account of the IPT implementation practices that have been successfully used to create a secure IPT-based network. Chapter V will provide a background of the Coast Guard's move to IPT at Headquarters Support Command. Chapter VI will apply the research to the Coast Guard's implementation by examining their deployment process and by making recommendations for improvement.

## C. COAST GUARD BENEFIT

The Coast Guard will receive the following tangible outputs from the research process: (1) a document providing security policy recommendations for IPT (Appendix A), (2) a manager's guide that provides recommendations for effective deployment practices of IPT-based networks in the Coast Guard (Appendix B), and (3) feedback on the implementation process and security measures being used to deploy IPT at CG Headquarters. The Coast Guard will gain an understanding of the advantages, limitations, and security issues that it will face as it considers further implementation of IPT.

# II. PUBLIC SWITCHED TELPHONE NETWORK (PSTN) AND INTERNET PROTOCOL TELEPHONY (IPT) OVERVIEW

## A. PURPOSE

The purpose of this chapter is to provide a basic understanding of the operation and functions of the Public Switched Telephone Network (PSTN) and of Internet Protocol Telephony (IPT). This will help to make comparisons between the two types of telephony in regards to strengths and weaknesses, reliability, and feature sets. It will also facilitate the identification of security vulnerabilities so that appropriate measures may be applied to mitigate the risks of potential threats.

## B. PSTN OVERVIEW

### 1. Background

The Plain Old Telephone System (POTS) has come a long way since Alexander Graham Bell’s first connection in 1876. A simple system, that required two endpoints to be physically connected to operate, has evolved into a complex switching system that allows people to communicate with others all over the globe at an affordable cost. This section will provide a very brief and simple description of how the PSTN operates and what types of services it provides. It is important to understand the capabilities of the PSTN because people will expect similar performance from IPT, especially when it comes to reliability and voice quality.

#### *a. Reliability*

We often take for granted the high level of reliability that our telephones provide. The well-established POTS provides redundancies that allow us to get a dial tone every time we pick up the phone, even during

power outages. Most people would not be able to clearly recall the last time they had a dropped call nor remember when they could not get a connection. This level of reliability is often referred to as “five nines,” that is, the telephone network is operational 99.999% of the time. This translates to about 5.256 minutes of downtime per year (Walker 3). Most believe that the telephone companies provide this advertised level of service, though some believe that aging equipment and the inability to follow maintenance standards (called Bell System Practices) have created an environment where reliability is beginning to falter (Estes Interview, 16 Dec 04). Regardless of the PSTN’s actual reliability, we know from experience that it is much more dependable than our data networks, which we lose access to on a regular basis (on average about 5 days and 11.4 hours out of the year based on an estimated network reliability of 98.5% (Walker 68-9)). If we plan to move voice over the data network via IPT, we must be prepared to find a way to advance towards the level of reliability that users have come to expect from the PSTN.

***b. Quality***

Like reliability, the voice quality of the POTS has been refined over the years to provide clear messages across the network. Voice quality is purported to be so good that you can hear a pin drop. The quality can deteriorate through the use of cellular phones, wireless phones, and satellite communications, but rarely does so over the physical network.

The most widely accepted method of evaluating voice quality is a subjective assessment called the mean opinion score or MOS. MOS is calculated by having several

human listeners rate the quality of a call on a scale of 1 to 5 and taking the average. Determining voice quality in this manner can be very expensive; as a result, several algorithms have been created to estimate voice quality and map their scores to the MOS model. The Mean Opinion Score Scale is shown in Table 1. A MOS of 4 or higher is considered toll quality, while values less than 3.6 usually result in user dissatisfaction (Walker 79-81).

| MOS | Quality Rating |
|---|---|
| 5 | Excellent |
| 4 | Good |
| 3 | Fair |
| 2 | Poor |
| 1 | Bad |

Table 1. Mean Opinion Score Scale (From Walker 80)

The MOS of a network (whether it be, for instance, the PSTN, IPT, or a Cellular network) is dependent on call volume, the type of compression used, and other network design factors. Generally, telephones on the PSTN provide toll quality service, while cell phones and IP Phones frequently fall short. To successfully imitate the PSTN, IPT must attempt to reach a consistent level of quality; however, consumers have been willing to accept lower quality in cellular phones to realize mobility and may consider similar trade-offs from IPT.

#### ***c. Features***

The PSTN provides a variety of services that we have become familiar with through residential use. Some of these include: Local, long distance, and international

service; Call waiting; Call forwarding; Three-way calling; Caller ID; Call blocking; Automatic callback; Call return (*69; Calling cards; Voice mail; Toll free numbers (e.g., 800) (Davidson 16-7). At home, we usually only use simple features to allow convenient voice communication and enable data connections to the internet. On the other hand, organizations find great business value in utilizing these features in a variety of ways. For instance, a company may use an 800 number and phone tree (enabled by call forwarding) to connect the customer to the right person, and use Caller ID as a piece of information to determine the customer’s identity. Businesses also leverage the power of the PSTN through conferencing and advanced voice mail services. IPT-based networks must provide, at a minimum, the same services and features (or suitable replacements) that a business already relies on from its POTS.

IPT must also provision for two other services that provide for the safety and security of individuals and governments, Emergency 911 (E911) and the Government Emergency Telecommunications Service (GETS). E911 is a service available to any user that provides the location of a phone to emergency dispatch services. The GETS is provided only to authorized individuals from certain government agencies and private companies that handle critical infrastructure recovery operations. GETS these personnel a higher probability of getting a dial tone during emergencies (e.g., earthquakes, hurricanes, terrorist attacks, etc.) when the PSTN becomes overburdened with calls (Carlberg 2-4). These services have been well-established on the PSTN and must be replicated in IPT.

### *d. Regulation and Cost Structure*

The PSTN is regulated to a degree (less so than in the years prior to deregulation in 1980) to ensure a stable infrastructure, mostly in the form of taxes, fees, and prescribed processes mandated by federal and local governments. Despite these regulatory costs (which are currently very limited with IPT), telephone carriers have been able to provide relatively cheap long distance services. Billing on the PSTN is relatively simple because carriers control large segments of the network and collectively own the entire network. Users are typically charged an access fee and additional charges for each unit (e.g., minute) of use. In contrast, billing for IPT-based networks is more complex because it is more difficult to track phone calls through multiple networks. Telephone carriers must work to create an effective billing system for IPT that addresses a complicated data network.

### *e. Common Threats*

The PSTN is a reasonably secure network due to years of experience and a strong physical infrastructure. The POTS holds most of its information in equipment that is physically protected, where access is limited to the general public. Though conversation confidentiality is not guaranteed (however, this risk is generally accepted by the public and mitigated by certain agencies through the use of encryption), private information is well guarded and the industry’s largest concern has been the threat of Phreaking. A Phreaker is similar to a black hat hacker who attempts to get free phone calls through illegal methods. IPT will be subject to the same risks present in the PSTN, but must also be prepared to address the threats introduced

by utilizing a network that could easily be accessed by almost anyone.

### 2. PSTN Operation

The POTS is made up of a variety of redundant and physically protected elements that create a very reliable (5 nines) and relatively secure (compared to voice over data network) telephone network. A list of the basic components of the network follows to help demonstrate how a voice conversation is carried across the PSTN.

#### *a. Components*

(1) Telephone and Circuit: The typical home handset is a simple device that sends and receives an analog signal (voice) to/from the local switch. Business telephones are often digital devices that connect to the company's Private Branch Exchange (PBX). The basic circuit from the telephone to the local switch is called a twisted pair. It is composed of two wires, twisted to reduce interference, and a sleeve used to transmit signals and voice at 48 volts. These components are commonly referred to as tip (negative wire), ring (positive wire), and ground (sleeve) (Newton 858, 837).

(2) Private Branch Exchange (PBX): The PBX is used by organizations to enable many features of the PSTN that are not necessarily available for residential service. It is similar to the local office switch that most residential users are connected to, but is located within and usually owned by the organization. It allows businesses to provide services for many users with fewer resources by sharing lines (but not phone numbers). They are often able to achieve further savings and functionality by connecting PBXs at different offices. The functionality of the PBX may be outsourced to the local service provider at a lower cost

to the company, known as Centrex, but usually comes at a loss of control of over some telephony components and features (Walker 9).

(3) Switches: The first two telephones had to be physically connected to function, and modern telephones require the same connectivity. Rather then physically connect every telephone to every other telephone, networks of switches were developed. These switches consolidate several lines together and create the physical connections required to link two phones. The first switch that a phone is connected to is usually the local switch or local office and is sometimes referred to as a Class 5 switch. At this point, the analog signal is converted to a digital signal and sent to the next switch on the network. These switches at the core of the network are called tandem switches and move large call volumes through the network (Walker 7-8).

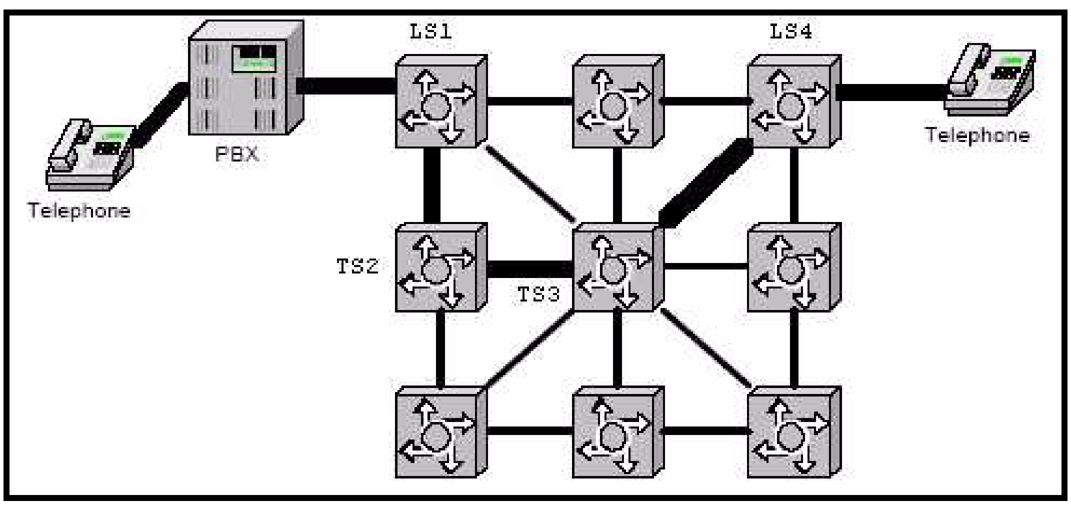


Figure 1. Circuit-Switched Network (After Ragsdale 2)

These switches form a dedicated circuit from one phone to another through the duration of a call as illustrated in the example in Figure 1. The call is initiated from a digital phone and connected to the PSTN

through the PBX. The voice signal moves from local switch 1 (LS1), through tandem switches 2 (TS2) and 3(TS3), to local switch 4 (LS4). The signal is converted to analog at LS4 and is received by the other caller on an analog telephone. The entire phone conversation takes place on this connection in both directions until the call is complete. Not all telephone connections are established this way, as many telephone carriers now have some sort of packet-switching located in the backbone of their networks; however, this type of connection is usually established for a local call.

(4) Trunk lines: Switches on the PSTN are connected by trunk lines. The capacity of a trunk line is measured by the number of channels it can hold. A basic channel, called digital signal level 0 (DS0), that supports one phone line requires 64 kbps of bandwidth to achieve adequate digital voice quality. A T1 (trunk level 1) line supplies 1.544 mbps to support 24 DS0 channels (and 8 kbps of overhead per channel) (Newton 800).

(5) Signaling System 7 (SS7): The components discussed to this point provide the basic physical connection from one endpoint to another. SS7 provides the means to set up, manage, and tear down a call so that information can flow freely between two telephones. SS7 is referred to as out-of-band signaling because it does not use the same path as the voice signal. In fact, SS7 utilizes switches that operate like the packet-switched internet. The SS7 is made up primarily of three components: The Service Switching Point (SSP), the Signal Transfer Point (STP), and the Service Control Point (SCP). The SSPs are usually located near the endpoint local switches of the PSTN. The SSPs usually generate and receive the signaling

messages to set up and manage voice circuits. The STPs are similar to switches, moving signaling messages through the SS7 network, and communicate with tandem switches and the destination local switch to setup a call. The SCPs provide the interface to databases that provide information for toll free number lookups and other call management features. These components are linked together in a network to provide an efficient method of setting up calls without tying up bandwidth on the voice network (Ragsdale 111-118). Figure 2 shows how these integrate into the system.

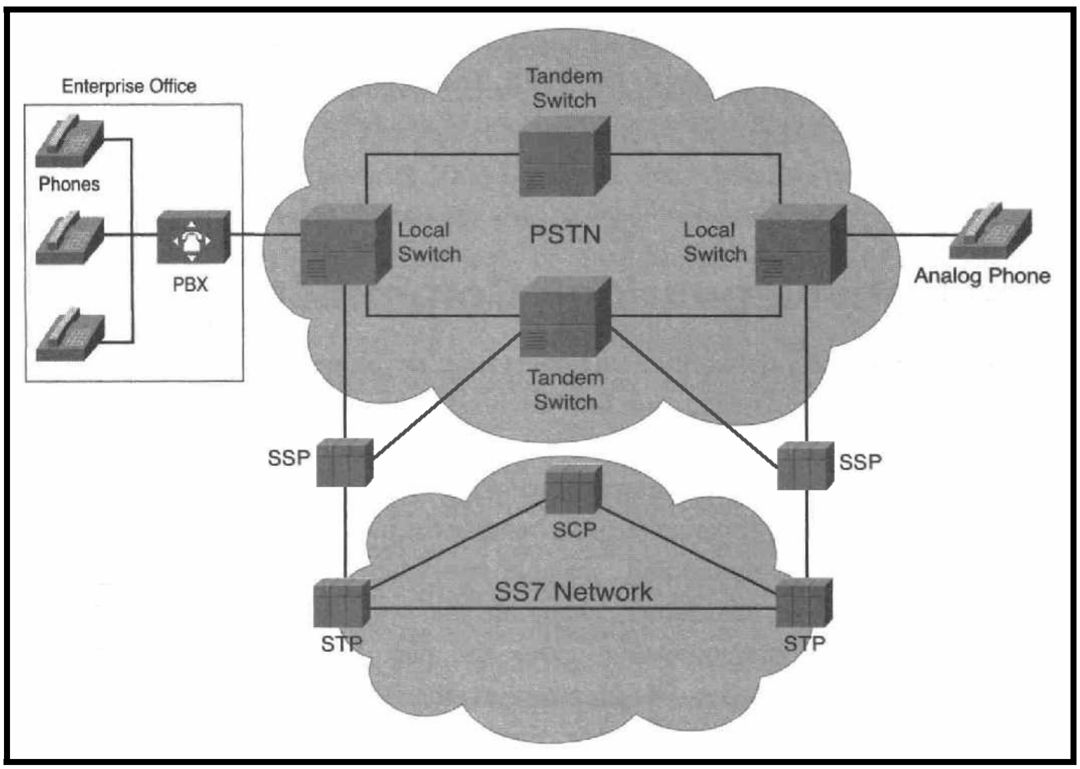


Figure 2. PSTN Diagram (After Walker 9, 11)

#### *b. Making a Call*

Figure 2 provides an illustration of how these basic components of the PSTN work together to make a call between two telephones (from an enterprise office to a residential phone in this example). First, the user picks

up the phone and hears a dial tone. The dial tone is generated by the PBX or local office to indicate that there is a connection and power to the local switch. When the user dials a number it begins the call setup process. The SSP at the local switch generates messages that are managed by the STPs to communicate with tandem switches and the other local switch on the voice network. The STPs will, by way of the SSPs, reserve a path for the voice conversation and alert the other local switch that a call is incoming. If necessary, the STPs will use the SCPs to look up the location of a number (e.g., 800 number lookup) or to retrieve other management information. Next, the local switch will signal the analog telephone to ring. When a user answers the telephone at the other end, a similar signaling process will occur to notify the telephone at the office to begin the conversation. Once the call is set up, voice is transported across the PSTN as described in section B.2.a(3) of this chapter. When either user hangs up to complete the call another signaling transaction, similar to the setup process, occurs on the SS7 Network to release PSTN resources.

## C. IPT OPERATION

### 1. Definition

A variety of terminology has been coined to describe the process of replicating the function of the PSTN by moving voice on data networks, including: Voice over Internet Protocol (VoIP or VOIP), Internet telephony, internet telephony, Voice on the Net (VON), next-generation telephony, computer telephony, packet telephony, intranet telephony, extranet telephony, etc (McKnight 3). As a broad description of all methods of moving voice over a packet-switched network, the author uses the term Internet

Protocol Telephony (IPT) to “refer to the components and technology needed to place telephone calls over an[y] IP-based network” (Walker 2). A description of the basic components and functionality of IPT follows.

**2. (Voice) Data Transport**

Although there are a variety of methods (discussed below) to set up and manage a call over data networks, all IPT phone calls share similar elements to transport voice data over packet-switched networks. These include: telephones, codecs, packet-switched networks and protocols.

***a. Telephones***

IPT telephones can take many forms. They may consist of simple analog phones connected to adapters that utilize bandwidth provided by an internet service provider (ISP). They may exist in the form of softphones, where a PC with a microphone and software are used to create a virtual phone. The most common IPT telephone, called an IP Phone, consists of a handset and a processor that provides varying degrees of IPT functionality depending on the model. The important point to note is that the intelligence of the network no longer resides deep within the network (as it does in the PSTN), but is often contained closer to or within the endpoints (Arkin, *Security*, 32).

***b. Codecs***

A codec derives its name from the process of coding and decoding. Codecs are used to convert an analog signal to a digital signal (code) and convert digital to analog (decode). This process may also include compression and other functions to optimize the signal bandwidth. The selection of a codec must be approached carefully to ensure good quality calls on IPT-based networks. A codec that does little compression will handle packets more quickly, but

will require more bandwidth. If there isn’t enough bandwidth, quality will suffer. On the other hand, codecs that do more compression take longer to handle packets and may potential lose information, creating potential drops in quality. When selecting a codec for a particular network, these concerns must be carefully balanced (Miller 254-256).

### c. Packet-Switched Network

The packet-switched network of the Internet differs significantly from the circuit-switched network of the PSTN. Where the PSTN dedicates one line to an entire telephone conversation, IPT splits the conversation into small pieces (called packets) and transmits them, via Internet Protocol (IP), over a variety of paths depending on varying network traffic conditions. These packets also share network resources, such as the bandwidth allotted to a network, unlike the PSTN which dedicates the line to the call’s use. This type of network provides a connectionless or “best-effort” approach to packet delivery, that is, packets are not guaranteed to reach their final destination. Figure 3 illustrates the movement of voice packets over a packet-switched network and provides a comparison with the circuit-switched network in Figure 1. Notice that the dark packets take different routes and share resources with other (white) packets on the network.

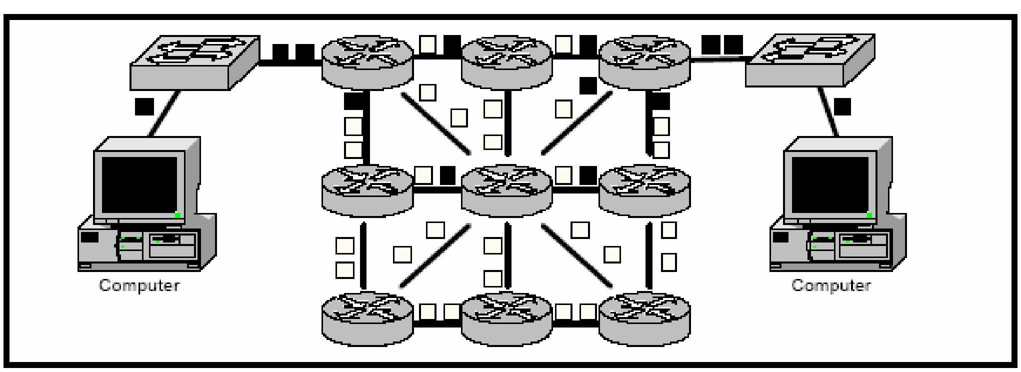


Figure 3. Packet-Switched Network (After Ragsdale 2)

The switch and trunk components of a packet-switched network are similar to those of the PSTN. Devices that provide for connections between nodes in the network are called switches, and devices that connect networks are called routers. The links (or trunks) between switches and routers are similar to those of the PSTN and propagate data packets via a variety of media (e.g., copper wire, fiber optic cable, wireless, satellite, etc.).

#### *d. Transport Protocols*

The Transmission Control Protocol (TCP), a connection orientated protocol, was developed to achieve better reliability from the best effort packet-switched network. Both ends of a communication ensure reliable information exchange by acknowledging receipt of packets. Lost or damaged packets can be re-sent and reassembled through this process to attain complete information. This process, however, requires too much overhead and is too slow for real-time applications like voice conversations. However, TCP is often used to carry higher-layer protocols that setup and tear down IPT calls.

The User Datagram Protocol (UDP), a connectionless orientated protocol like IP, is a simpler protocol than TCP and is used where reliable transmission of every packet is not critical. UDP has much less overhead and does nothing to acknowledge or resend packets. This protocol is useful when transmitting real-time data, such as multimedia video and audio, because even if it was determined that a packet was not received, it would be too late to resend the packet since the stream of audio or video would have passed the point that it could be reinserted. Though packets may be lost, it is usually

acceptable since a single lost packet would not significantly affect the transmission of the information, and its use is usually limited to a robust network where loss would be minimal. IPT utilizes UDP to transport voice conversations because, even though it does not guarantee delivery of every voice packet, it provides better quality than the inherent delay created by TCP.

Real-Time Transport Protocol (RTP) is a higher-layer protocol that is encapsulated in UDP and is specifically used to support streaming real-time multimedia applications like IPT. RTP carries the bulk of the voice conversation between two IPT endpoints once a connection is established. It provides support for "content identification, timing reconstruction, loss detection and security" (Newton 717). It is supported by the Resource Reservation Protocol (RSVP) to enable Quality of Service (i.e., prioritization of voice packets).

The components discusses above provide a basic overview of the elements that facilitate the movement of the actual voice conversation in IPT. After the call is established, a user speaks into the phone, the analog voice signal is converted to a digital signal that may be compressed, and the signal is split into packets and carried over the packet-switched network via Internet protocols.

### 3. Signaling Protocols

A variety of protocols exist that set up and manage telephone calls in the IPT-based network. These protocols have been created by different standards bodies and by commercial organizations that developed their own propriety protocols (e.g., Cisco's Skinny Client Control Protocol).

Varying protocols have created an environment where interoperability among IPT-based networks is difficult, but many believe that one standard will soon emerge. A brief description of two of the most commonly used IPT signaling protocols, Session Initiation Protocol (SIP) and H.323, will be provided to understand call setup.

***a. H.323***

The H.323 standard, developed by the International Telecommunication Union (ITU-T), encompasses a set of standards designed to enable real-time multimedia (voice, video, and data) communications over a packet-switched network. This is one of the first protocols developed for IPT and is currently the most widely supported. The high level of detail of the standard provides for excellent interoperability but has high overhead and is slow to change (Passmore, *SIP*, 9).

(1) Components: H.323 has four primary components: Terminal, Gateway, Gatekeeper, and Multipoint Control Unit (MCU). The terminals represent the endpoints, telephones in the case of IPT. Gateways are optional and provide connections to other networks, protocols, or formats (e.g., PSTN). Gatekeepers are also optional, but if present must be used to provide address translation and manage calls to control bandwidth. The MCU is used to conference three or more Terminals or Gateways (Newton 383). Figure 4 displays how these components fit together and connect to other networks in the H.323 architecture.

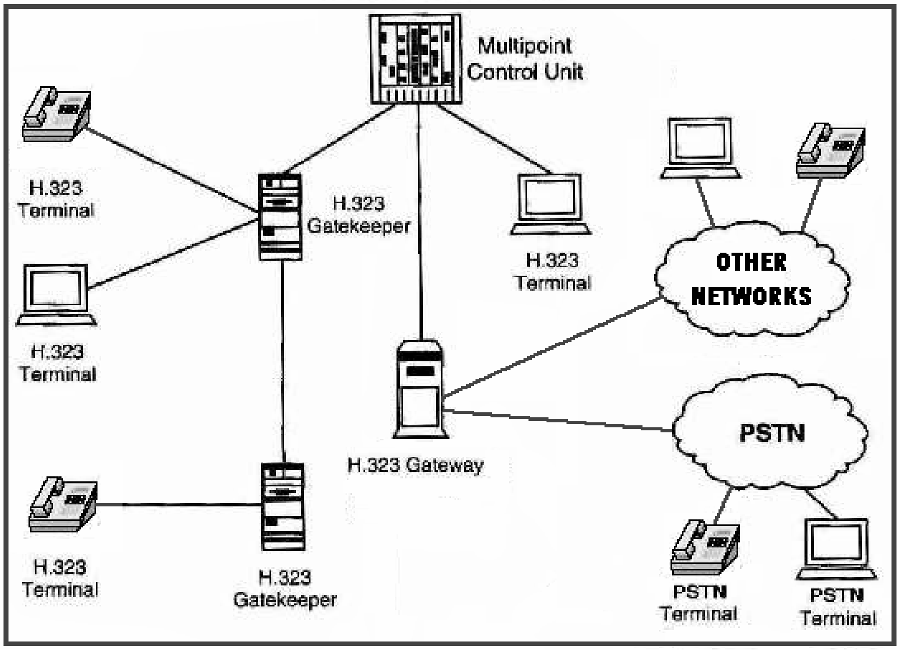


Figure 4. H.323 Architecture (After Miller 217)

(2) Command and Control Protocols: H.323 is considered an umbrella standard over several protocols, but only three of the primary protocols used by H.323 will be discussed here: H.245, Q.931, and RAS (Registration, Admissions, and Status). H.245, a call control channel, is used to send control messages to negotiate a terminal's capabilities. Q.931 sets up connections between terminals. RAS is used to setup connections and manage communications between any component and gatekeepers. RAS is not utilized if a gatekeeper is not present (Newton 383).

(3) Placing a Call: An example of a basic phone call, between two terminals that share the same gatekeeper, such as two phones on the same Local Area Network (LAN), is illustrated in Figure 5. Prior to the call, both terminals must register with the gatekeeper by exchanging RAS messages with the gatekeeper. When placing a call, terminal 1 will request bandwidth and terminal 2's address from the gatekeeper. After the gatekeeper

acknowledges the request, terminal 1 will contact terminal 2 directly to negotiate session parameters. If terminal 2 accepts the call, it will also request bandwidth from the gatekeeper. After receiving an acknowledgement, terminal 2 will notify terminal 1 and voice conversation may begin. Concluding the call is conducted in a similar manner in order to release bandwidth.

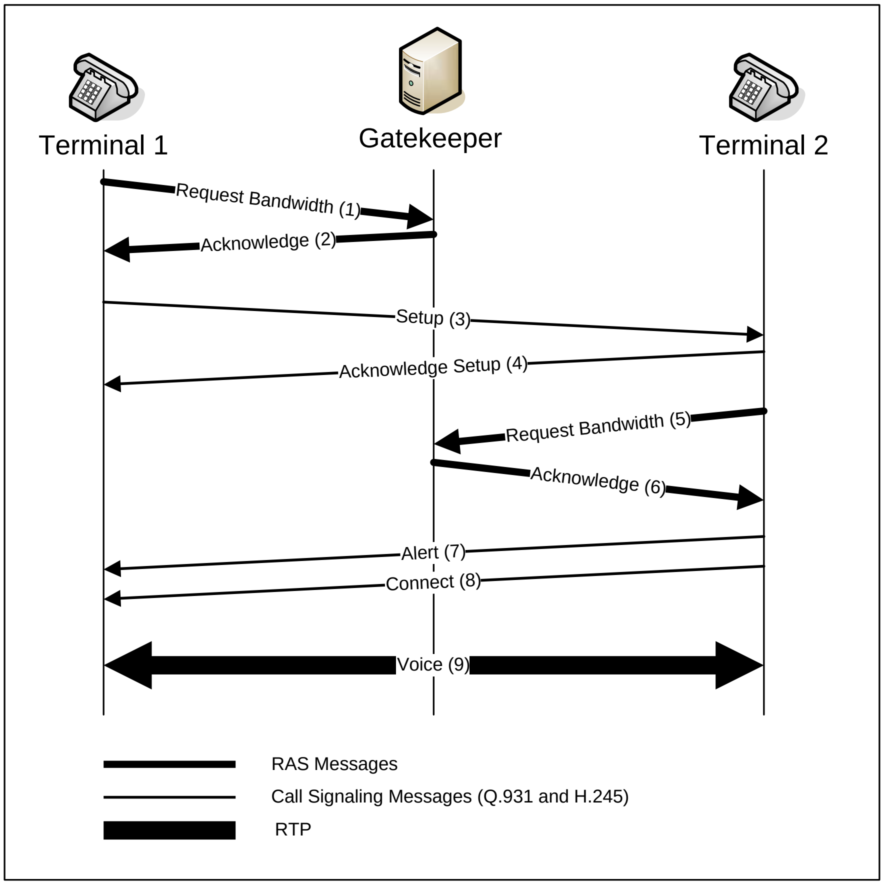


Figure 5. H.323 Call Signaling (After Miller 225)

#### *b. SIP*

Session Initiation Protocol (SIP) was standardized by the Internet Engineering Task Force (IETF) in 1999 as Request for Comment (RFC) 2543. The protocol was designed with simplicity in mind, focusing on session initiation and termination, while relying on other Internet Protocols (such as TCP, UDP, RTP, and Session Description

Protocol) to complete the process. SIP is much like HTTP, using text-based messages to setup call connections. This “lightweight” protocol is expected to dominate the industry because it facilitates quick, scalable IPT solutions and creates the potential for a variety of features that the PSTN or H.323 are too slow to provide.

(1) Components: SIP-based networks consist of two main components, User Agents and Servers. User Agents (UA) are endpoints (e.g., IP telephones) that contain a Client (UAC) and a Server (UAS). The UAC initiates requests and the UAS responds to requests. There are several SIP servers that provide certain services on the IPT-based network. Proxy servers make requests in behalf of other clients, Redirect servers provide address translation, Register servers register clients on the network, and Location servers provide the call recipient’s possible location to other servers. SIP components are identified with Uniform Resource Locators (URL) to simplify addressing. See Figure 6 for how these components reside within a network.

(2) Placing a Call: Figure 6 shows an example of how the components of a SIP network are used to initiate a call {note: Prior to the call, the UAs will have already registered with a Registration server}. (Step 1) When the telephone (UA) is picked up, and the number dialed, an Invite request is sent to its Proxy server. (Step 2) The Proxy will query the Redirect server (could have queried a Location server as well) for an address of the called party. (Step 3) The Redirect server responds with an address to the call recipient’s network. (Step 4) The Proxy server sends an invite to the second Proxy server through the IP Network. (Steps 5-6) The second Proxy server

will query a location service that is not necessarily SIP and receive the address of the called party’s Proxy server. (Steps 7-8) The second Proxy server will send an Invite request to the third Proxy server that will then notify the call recipient that the caller desires to setup a connection. (Steps 9-12) When the called party picks up the phone, the UA will then acknowledge the Invite request back to the caller via the Proxy servers. Once a call is established, voice will flow via RTP as described above. The call will be terminated in a similar fashion, but will not require the services of the Redirect or Location Servers.

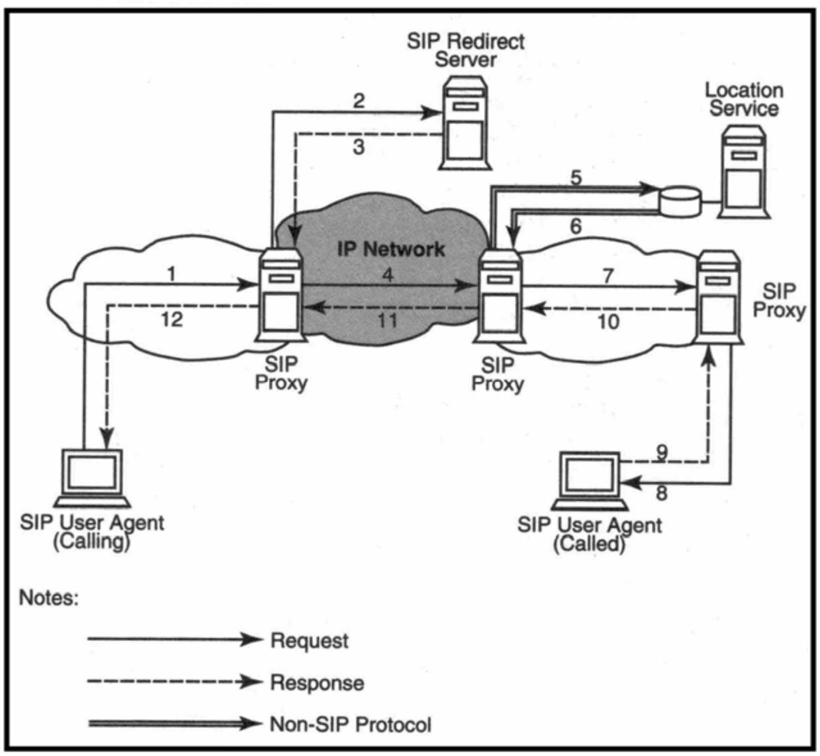


Figure 6. SIP Network Architecture (From Miller 232)

### 4. Voice Quality

The process of moving voice over the data network as described above presents some challenges for maintaining high levels of voice quality. An explanation of some of

these issues will be related to help understand what kind of factors cause voice quality to improve or to deteriorate.

### *a. Latency/Delay*

Latency or delay is the amount of time it takes for voice to travel from the speaker's mouth to the receiver's ear. Delay can be categorized in three ways: as propagation delay, handling delay, and serialization delay. Propagation delay is the amount of time it takes for the data to traverse the medium (e.g., speed of light through optical fiber) it is carried on. Serialization delay is the time it takes to place a bit onto an interface (bit rate), but is usually ignored, as it is relatively small with modern equipment. Handling delay is created by the equipment that processes data packets as it traverses a network. It commonly occurs in codecs where analog/digital signals are converted and data is compressed. Firewalls, switches, and routers create some delay while reading packet or header information and deciding how to process the packet. When networks are congested, the packets also see an increase in latency while waiting in queues. To provide an acceptable level of quality, the IPT-based network *must not have delay in excess of 150 ms*, and must reduce delay even further to meet the quality provided by the POTS (which is mostly affected by propagation delay, and minor handling delay (Davidson 167-169).

### *b. Jitter*

Jitter refers to variations in the arrival time and order of packets. Jitter can potentially cause packets to be assembled out of sequence or to be dropped. To allow for non-uniform arrival times, jitter buffers are configured to wait a set amount of time before assembling

packets. This adds additional delay and must be balanced with the potential of losing packets that don't arrive within the buffer timeframe (Kuhn 20-21).

***c. Lost Packets***

Lost packets are those packets that are dropped in the network, whether it is from improper routing, corrupted data, overflowing queues, or late arrivals. IPT can accept a certain amount of packet loss (approximately 1-3%) without negative affects because the packets are so small (10-50 bytes); however, packet loss is often a bursty behavior, where many packets are lost at once (Kuhn 21-22). The solution to this problem usually involves good management of network resources, which will be discussed in implementation practices in Chapter IV. Another option considered to remedy this problem is to send redundant information, causing an increase in bandwidth.

***d. Echo***

Echo is created when the receiver's telephony equipment amplifies and returns parts of the original signal back to the sender. It negatively impacts the conversation when the delay is greater than 25 ms. It can be reduced by properly configuring echo cancellers that are equipped with most IPT devices (Davidson 175).

***e. Quality of Service (QoS)***

QoS refers to services that give priority to certain packets, such as time-sensitive IPT packets over web browser traffic, to improve the affects of packet loss, jitter and handling delay. A variety of protocols are in use or being planned to help prioritize real-time data flows. They give priority to packets from time sensitive applications like IPT, subsequently slowing the processing of other information flows where time is less critical

(like email). Several companies provide tools to help monitor and manage QoS to balance the needs of applications and bandwidth constraints. The use of QoS mechanisms is considered a must to successfully attain good call quality on data networks.

#### ***f. Bandwidth***

Increased bandwidth is often seen as the solution to many of the delays created in a packet-switched network, but data networks quickly consume increases in bandwidth. Increases in bandwidth will help to prevent packet loss, jitter, and decrease delay, but the best network performance is achieved by managing bandwidth rather than constantly increasing it.

#### ***g. Voice Activity Detection (VAD)***

VAD is used to detect pauses in speech to reduce the amount of bandwidth required to send voice conversations. The process saves significant amounts of bandwidth but can sometimes cut off the beginning of a phrase and will not work in noisy environments.

#### ***h. Security***

Implementing security measures will often introduce delay in the system. Firewalls and encryption, for instance, will increase handling delay in an IPT-based network. Security will be discussed in depth later, but it will become apparent that security often comes at a cost of voice quality.

## **D. BRIDGING PSTN AND IPT**

The telephony processes thus far have only addressed the PSTN and IPT in isolation. It is necessary to understand the interface between these two systems (and other systems like ISDN and Frame Relay Networks) to be

able to identify potential vulnerabilities in their interaction in later sections.

### 1. Components

The European Telecommunications Standards Institute (ETSI), which has cooperated with the ITU and IETF, has developed a model for communication between gateways of dissimilar networks. This model (see Figure 7) separates gateway functionality into three elements: a Signaling Gateway (SG), a Media Gateway (MG), and a Media Gateway Controller (MGC). Sometimes these components exist in one piece of hardware, but frequently they are controlled by several different organizations. The SG controls signaling functions between the IP network (e.g., SIP) and circuit-switched networks (e.g., SS7). The MG controls the media transfer between the IP network (e.g., RTP) and circuit-switched networks (e.g., pulse code modulated voice). The MGC coordinates call processing functions between the SG and MG by using either the MGCP or the MEGACO/H.248 protocols (Miller 237).

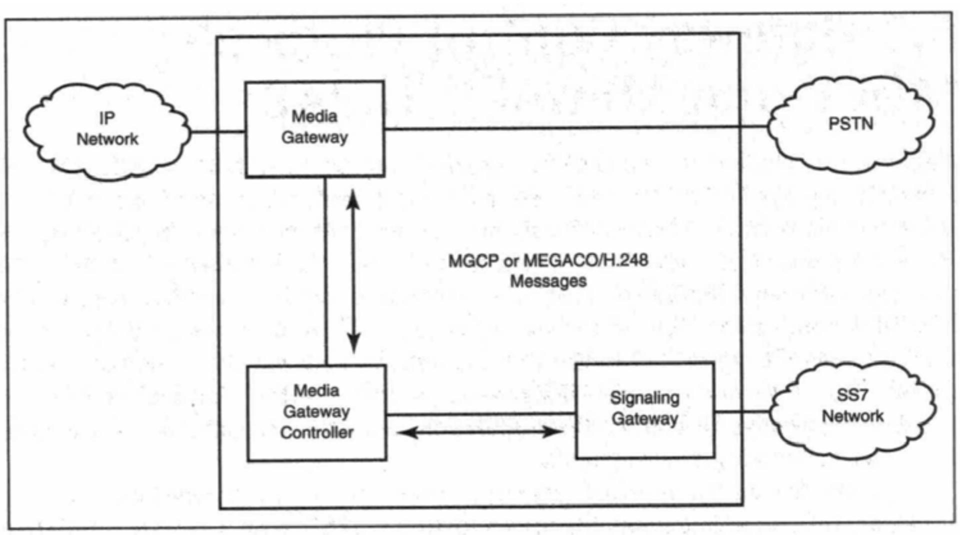


Figure 7. Gateway Architecture (From Miller 238)

### 2. Protocols

#### *a. Media Gateway Control Protocol (MGCP)*

MGCP was developed by the IETF in RFC 2705 and was one of the first standards used to provide interfaces between the PSTN and IP network. MGCP refers to MGCs as Call Agents and has different gateways that provide interfaces between IP networks and a variety of other networks. For instance, “trunking gateways” manage many digital circuits to connect the PSTN to an IPT-based network, “business gateways” connect PBXs to IPT-based networks, and “residential gateways” provide an analog connection to the IP network via cable modems and other devices. The MGCP uses Call Agents to define connections among two endpoints and manages those connections with MGCP commands that are transmitted via UDP (Miller 238-239).

#### *b. Media Gateway Control (MEGACO)/H.248*

This protocol was developed jointly by IETF and ITU to improve upon MGCP, although the two protocols are not interoperable. MEGACO’s architecture is similar to MGCP, but handles control somewhat differently and provides more features for better security and scalability. For the purpose of this document, MEGACO follows the same basic model as MGCP.

#### *c. SIP and H.323*

SIP and H.323 provide some basic functionality to interface IPT-based networks to the PSTN (via H.323 or SIP gateways) but are not widely used for this purpose.

### 3. Placing a Call

Figure 8 can be used to demonstrate how a call can be made from an IP telephone to an analog line on the PSTN. When the caller picks up the phone on the IPT-based network, it initiates the H.323 or SIP signaling process

described above. The H.323 or SIP gateway on the edge of the network communicates with the Call Agent to set up the call. The Call Agent communicates with the SS7 network via the Signaling Gateway in the MEGACO architecture. The SS7 network will contact the called party and initiate a connection if they answer the phone and pass an acknowledgement back to the IPT-based network via the Call Agent. The Call Agent will send a message to the Media Gateway to prepare for the transport of voice through the network. After the signaling process is complete, data will flow via the RTP: from the IP telephone, to an H.323 or SIP gateway, to the Media Gateway, to the PSTN network, and to the analog telephone. A call is terminated in a similar fashion to the setup and is initiated by hanging up.

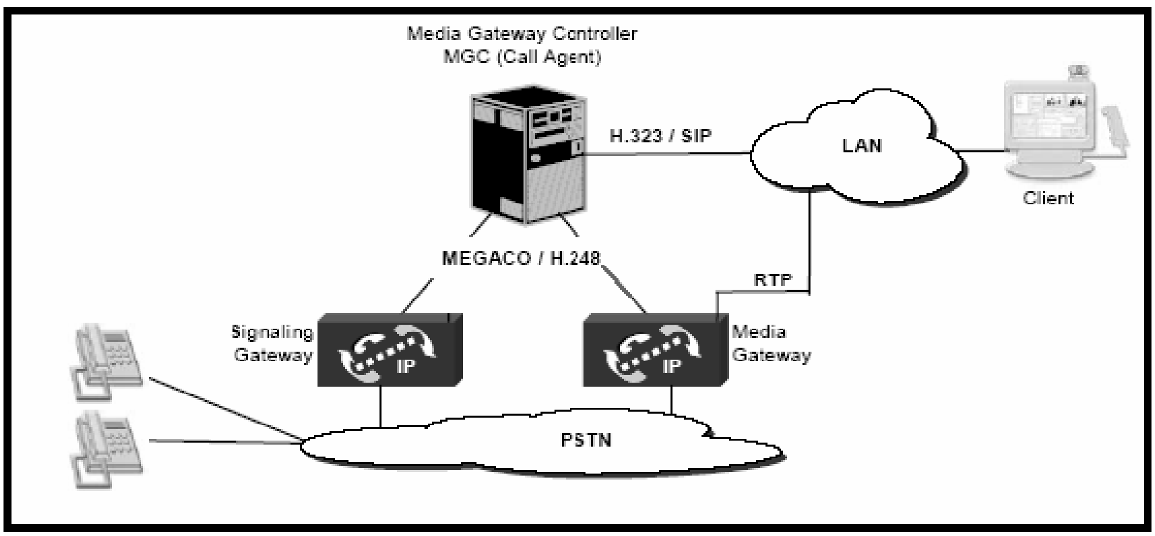


Figure 8. MGCP/MEGACO/H.248 Architecture (After Kuhn 48)

**4. IPT Architectures**

There are several IPT-based network designs that provide varying levels of IPT capability and network control to an organization. The following four are considered:

- **Broadband services**: These are services that are typically used by residential customers to save on long distance phone calls. They rely on a users existing broadband connection to provide service over the Internet. Services vary. For instance, among other services Vonage supplies its users with Analog Telephony Adapters that allow them to connect their traditional phones to their home routers. Other services, like Skype, are peer-to-peer services that require common (free) software between two users.

- **IP-PBX**: This is similar to the PBX described for the PSTN, except that it supports an IPT-based network within the organization. It is connected to the PSTN through a dedicated trunk.

- **IP-enabled PBX**: This is a hybrid solution, where a circuit-switched PBX is provided with interfaces for IPT equipment. It allows an incremental introduction of IPT without losing the features of the current PBX.

- **IP Centrex**: A local service provider supplies the core IPT services for those organizations that wish to save costs on equipment and space. The disadvantage to this approach is that fewer features are available and businesses have less control of the network, making it more difficult to make changes or protect information.

**E. WHY IPT?**

IPT has been around for a while, but did not originally see much use due to bandwidth constraints that prevented good voice quality. Thanks to rapid increases in processing speeds and bandwidth, IPT has become a feasible alternative or complement to the PSTN. Despite IPT’s

inability to consistently provide the same level of voice quality and availability as the PSTN, it has grown to provide other forms of value, through lower costs, convergence, and enhanced feature sets, that the PSTN cannot. As voice quality and network reliability improve, many organizations are beginning to see fewer tradeoffs to IPT implementation.

**1. Lower Costs**

Many believe that IPT provides a means to make virtually free long distance and international calls, especially within an enterprise network. These savings are enabled by increasingly cheap bandwidth and by a lack of regulation (i.e., taxes) on media transport over internets. The bandwidth even becomes cheaper when comparing the required 64kbps throughput dedicated to a call on the POTS to the 14 kbps used for an IPT call (Varshney 90). However, most of these savings are not as large as publicized due to the relatively low cost of long distance, the cost of replacing PSTN components, and the cost of upgrading network components to support IPT.

> Toll-call savings are of minor interest to government agencies that already enjoy economies offered by government wide telecommunications contracts. Lower costs alone don’t justify significant investments in IP telephony and related network upgrades (Joch,*IP telephony*).

Most would agree that the motivation to shift to IP is no longer driven by direct cost savings, but by other benefits.

**2. Convergence**

A significant benefit of shifting to IPT is the potential to consolidating the voice and data networks into one network, which is known as convergence. Organizations

can find great value in building one physical infrastructure. After the initial setup costs, maintenance and upkeep will become cheaper as less equipment will need to be maintained. Training and staffing costs will also fall because businesses no longer have to maintain two separate networks. Initial barriers to network convergence are caused by the high cost of replacing old systems and security risks. These roadblocks are slowly diminishing as PSTN systems age and require replacement and as security professionals more closely address the vulnerabilities of a converged system.

### 3. Enhanced Feature Sets

One of the greatest motivators to pursuing IPT implementation is the number, ease, and scalability of features that IPT systems are expected to provide. They have already proven their value by imitating most of the features that we have come to expect from the PSTN. The capabilities of the IPT protocols are easy to use and implemented quickly, far surpassing the sluggish change processes required with the PSTN. This has been demonstrated, for instance, with how quickly Moves, Adds, and Changes (MAC) can be performed. On the PSTN it could take as long as a few weeks to have a person’s phone moved to a new location and reconfigured, often at substantial cost. The slow response was often a result of sloppy wiring closets and the need for administrative assistance. On the IPT-based network a telephone can be moved within moments without the need of administrative control, because configuration capabilities lie within the IP phone and because no physical changes are required. Another powerful tool that businesses are utilizing is Unified Messaging Systems (UMS), where email and voice are converging to a

single mailbox allowing users to access their messages and communicate with colleagues in different ways. These are several examples of new capabilities that organizations are using to improve productivity, add value to business processes, and serve customers. It is expected that SIP will continue to enable rapid growth and implementation of new features.

## F. IPT CHALLENGES

A shift to IPT produces significant benefits, but introduces risks that must be addressed and mitigated. By combining voice with data, we introduce the same security vulnerabilities to our voice systems that already exist on the data network, weaknesses that were nonexistent or sufficiently minimized in the PSTN. New interfaces between the PSTN and IPT are also likely to expose our networks to new threats. Understanding the operation of IPT and the functionality it attempts to emulate from the PSTN will help us to recognize points of vulnerability in the IPT system. The potential security risks introduced in this new environment will be discussed in-depth in the next chapter.

Along with security issues, we find that voice quality and system availability may decline when shifting to IPT. An organization must carefully balance its management of IPT resources, as we are likely to find that an increase in quality is often associated with a decrease in security or an increase in costs. Other challenges include regulatory issues such as wiretapping under the Communications for Law Enforcement Act of 1994 (CALEA) on the one hand, and protecting private or proprietary information on the other. As organizations make the decision to implement IPT, they must carefully weigh the associated gains and tradeoffs. In

the long run though, we are likely to see companies discover that the greatest value will be located in a converged network.

# III. IPT SECURITY

## A. PURPOSE

This chapter provides descriptions of the most common security risks to IPT and the tools used to mitigate them. It includes a discussion of the costs (not necessarily in dollars) associated with either implementing security measures or ignoring the risks, in light of the common technique to measure the effectiveness of a network’s security in terms of Confidentiality, Integrity, Availability, and Authentication. Finally, a review of the U.S. Coast Guards current information technology policies is presented, and potential IPT security policy gaps are identified.

The material in this chapter uses concepts (threats, vulnerabilities, and consequences) of a risk model presented by William Murray, to help gain an understanding of how to balance security risks with effective safeguards. Threats are attacks on the system and are usually measured as a rate of occurrence. Vulnerabilities are weaknesses in the system that either exist (value of 1) or do not exist (value of 0). Consequences are the costs (e.g., time, money, reputation, etc.) that an organization incurs when an attack is successful. Multiplying these factors together can give a company a quantifiable (or subjective) estimate of risks and balance them with the costs of security mechanisms (Murray Notes).

$$\boxed{\text{Risk} = \text{Threat}_{(\text{rate})} \text{ X } \text{Vulnerability}_{(1,0)} \text{ X } \text{Consequence}_{(\$,\text{Time},\text{other})}}$$

Figure 9. Risk Model

A simple example of how this model could be used follows, but the process of examining risk may vary in scope and detail depending on the needs of the organization. A company endeavors to determine the risk of spam (junk mail). The business is vulnerable (V=1) because it receives all mail from any recipient. Employees encounter spam every business day of the month (T=20/month). On average, employees spend about five minutes per day sorting through junk mail(C=5 min/day). The risk that the company currently accepts each month totals about 100 (20*1*5) minutes of lost productivity per employee. Assuming that each employee is paid $.25 per minute ($15/hr), the company loses $25 of productivity for each employee per month. To reduce this cost, the company considers purchasing and maintaining a spam filter that costs about $5 per month per employee to maintain. The company will still receive spam everyday, but reduces it to the point where it only requires 1 minute per day to sort through, reducing lost productivity to 20 minutes or $5. The spam filter actually creates an additional vulnerability by blocking legitimate mail. The company estimates that it will require approximately 30 minutes ($7.50) of additional work per month for each employee to make up for missed correspondence. The total risk accepted by the organization after installing the spam filter would be equal to the cost of the safeguard ($5) plus the cost of the remaining security weaknesses ($12.50) for a total of $17.50. This analysis allows the company to determine that the spam filter will add more value to the company by reducing risk.

It is clear from the example that the model does not always provide a perfect answer because several assumptions must be made to determine risk. However, real value comes through the ability to analyze security weaknesses and safeguards, to compare various solutions, and to establish where the businesses priorities lie. This chapter helps to identify: vulnerabilities that are common to IPT-based networks, common or frequently occurring threats and their consequences, infrequent threats (e.g., natural disasters) with large consequences, and the safeguards used to mitigate the subsequent risks. Each organization must determine for itself how to balance each of these elements to provide the most value to the company.

## B. SECURITY THREATS

Security threats are those actors that interact with networks to degrade system security. Human threats and natural occurrences are introduced. IPT-based network managers must be aware of these threats to properly implement physical and logical barriers via safeguards.

Human threats to the network come in a variety of forms. Those people who work to circumvent security measures are often referred to as hackers. “White-hat” hackers claim to improve security by identifying holes and alerting those who can fix them. This can still be a threat if the bad guys hear of the fix before you do. “Black-hat” hackers (a.k.a. crackers) have criminal intent, whether it is for financial gain, notoriety, political gain, information warfare or other goals. From this point forward the author refers to all attackers, with malicious or criminal intent, as hackers. “Phreakers” are telephony hackers who specifically focus on receiving free phone

calls. The hackers described have varying levels of experience, from the teenager that downloads scripts off the Internet to the seasoned IT professional.

The human threat to computer systems is difficult because of three main advantages that computer criminals have: automation, action at a distance, and technique propagation. Automation is used to complete monotonous redundant tasks at high speeds (sometimes slowed to avoid detection). This ability allows the attacker to perform exploits that would normally be infeasible for an individual. Hackers are also able to perform attacks from a distance, leaving little to no physical evidence, and often crossing jurisdictional boundaries to avoid prosecution. Finally, numerous computer criminals are able to utilize the genius of individuals through technique propagation. That is, once one person has discovered a hole in security, the knowledge quickly spreads and can be used by anyone with minimal understanding (Walker 238-239).

The most dangerous of human threats exist from insiders, those personnel who work for the organization that is attacked. According to a survey of large companies and government agencies in 2000, over 80% believed that insiders where a likely source of attack which was higher than any other suggested source of attack (Power 160). These people usually have special knowledge or physical access that enables an attack that would have otherwise been unsuccessful from an outsider’s perspective. Insider threats can also be unintentional in the case of human error and complacency. Simple errors or failure to adhere to security policy (e.g., Failing to change default

passwords or leaving passwords lying around.) can often lead to breaches.

Threats to security are not all created through human interaction, but can often be caused through natural events. Fire, flooding, power outages, earthquakes, hurricanes, and other natural disasters can cause the network element failure and information loss. Extremes in humidity, heat and cold are also sources of failure. All of these potential threats must be assessed and planned for when created IPT security policy.

## C. IPT VULNERABILITIES

This section identifies common weaknesses in the IPT-based network that potentially enable system exploits. Where appropriate, the vulnerabilities will be compared with the level of protection provided by the PSTN.

### 1. Network Convergence

Not only does network convergence provide many of the benefits previously discussed, but it also supplies the source of many security weaknesses. When joining the data and voice networks, the telephony elements may become affected by the known (and unknown) vulnerabilities of the data network, and vice versa. This convergence also brings the signaling and data transport components of telephony together onto a common system. The generally isolated PSTN, with its separation of signaling and voice transport networks, is generally thought to provide a more secure environment. Convergence also introduces other risks to telephony, discussed below, due to its interaction with the operation and design of packet-switched internets.

### 2. IPT Protocols

IPT relies on internet protocols (e.g., TCP/IP, UDP, RTP, etc.) to perform signaling and transport data. The security risks inherent in these supporting protocols transfer into the IPT domain. Furthermore, many have observed that internet protocols are often designed with functionality first and security mechanisms later; including IPT protocols like SIP. This is in stark contrast to the well-established and closely regulated protocols of the PSTN.

Fortunately, SIP, H.323, and MEGACO/H.248 continue to be updated to include better security mechanisms. Two issues, however, that have not fully been addressed with these protocols are the use of Firewalls and Network Address Translation (NAT). These are very common security measures (to be discussed in more detail later) that complicate the use of IPT protocols. Those who implement IPT sometimes find that increased IPT functionality comes at a cost to the level of security provided by Firewalls and NAT.

### 3. Network Control & Placement of Intelligence

While the boundaries of the PSTN are easily identifiable and controlled, the limits of an IPT domain are often obscure. No single authority controls the IP medium; therefore, a voice conversation may flow through a variety of networks that are not necessarily controlled or trusted by the IPT user. Depending on the IPT implementation, this could potentially expose voice packets to unwanted contact. The Internet is more easily accessible than the PSTN and allows access to information that isn’t as easily reachable on the PSTN.

Relative to data networks, limited access to the PSTN has been possible because the information or intelligence of the network tends to reside in equipment that can be locked up and physically protected by telephone companies and organizations. This prevents access by the general public and makes it more difficult for malicious parties to attack the network. Even if we assume that the core components of the IPT-based network have the same physical protection as the PSTN, the IPT-based network will be vulnerable to the intelligence that resides at the end-points (i.e., IP phones, softphones, etc.). SIP, for instance, can provide IP phones with the ability to interact with other components (e.g., e-mail and voice application servers) of the IPT-based network which may allow greater manipulation of system devices. On the POTS network, most (but not all) telephones are considered “dumb terminals” that typically only allow communication with the local switch. It is no longer sufficient to protect switches and servers, but telephones themselves must be guarded (Arkin, *E.T.*, 13-14).

#### 4. IPT Components

Any piece of equipment in the IPT-based network can become the target of an attack. As illustrated above, some of these devices require different kinds of protection than equivalent portions of the PSTN. IPT Servers, gateways, network interfaces, and end-points require special attention to ensure appropriate security mechanisms are in place. It is also important to ensure that other protected data network components, like firewalls, switches and routers, have security mechanisms that do not inhibit the flow of voice packets.

### 5. Availability

As discussed earlier, the PSTN provides a high level of reliability or availability. The “five nines” of reliability provided by the POTS means that most of the time you are going to get a good quality call without any connection problems, even in cases where power is down. Data networks do not promise the same level of availability. Network congestion and outages are common on data networks and are tolerated to a certain degree; however, an IPT-based network must have better reliability in order to serve the needs of the organization. An attack directed at shutting down or slowing the data network will disrupt telephone service, a threat that is not present on the PSTN. Even natural occurrences that cause power outages are likely to interrupt IPT service where the POTS provides power to the line for telephone calls. IPT-based networks must be prepared to implement the redundancy required to achieve levels of reliability that meet the needs of the user, which is not necessarily the same as is currently supported by the PSTN.

### 6. PSTN Exposure

The interfaces between IPT-based networks and the PSTN (or other circuit-switched networks) create a potential point of vulnerability for both networks. It is common for organizations to utilize both the PSTN and IPT-based networks for their business processes. They must be careful to ensure that the security that they have come to expect from the PSTN is not compromised through its connections to a packet-switched network, and ensure that data network personnel recognize the potential threat of unfamiliar attacks on the PSTN that bleed over to the data network.

## D. IPT ATTACKS & CONSEQUENCES

Now that potential areas of IPT weakness have been enumerated, we can discuss some of the more common methods of exploiting them and the impact that successful attacks have on the network. A partial list of specific attacks that threaten IPT is provided in Table 2 to facilitate the discussion. There are an abundance of tools that hackers use to attack data networks, and many of them become potential threats to the IPT-based network. However, the focus of this discussion will center on common IPT attacks present in the data network and attacks that are distinct to the IPT environment.

### 1. IPT Phone Service Disruption

An attacker has a variety of methods to reduce the availability of an IPT-based network. Degraded availability in this case can refer to poor voice quality, the inability to connect with or receive calls from a desired party, or complete loss of telephony service. Depending on the needs of an organization, an attack on the availability of telephone services can cause minor irritations and inconveniences, create significant losses in potential revenue and competitive advantage, or increase life threatening risks.

A common method of attack on a data network to disrupt service is called Denial of Service (DoS). An attacker can use a variety of techniques to overwhelm network equipment, such as servers, with so much unnecessary data that the devices are unable to serve legitimate users. This can cause minor delays, and a subsequent drop in voice quality, or destabilize equipment to the point where it shuts down or fails to process any information.

| Attack | Description | Consequences |
|---|---|---|
| Virus | Malicious code usually spread by the user when executing a program. (e.g. opening a file) | Damage can vary from harmless and annoying (e.g. changes desktop background) to complete system compromise (e.g. system shuts down, lost/damaged files, back door installed). Viruses among IP Phones are not common, yet. |
| Worm | Malicious code that quickly spreads on its own. | Similar to Virus consequences. |
| Trojan horse | Malicious code implanted in seemingly innocent, but untrustworthy, programs. | Similar to Worm and Virus consequences. |
| Buffer overflow | Caused by poor coding practices. When a program allows inputs (e.g., 500 chars) that exceed the allotted memory (e.g., 8 chars), it can overwrite blocks of memory and have unintended consequences. | "The most common form of security vulnerability in the past decade" (Newton 130). Usually used to gain access to a piece of equipment or cause a system crash. The Morris worm, a buffer overflow exploit, caused over 6,000 servers to crash in 1989, bringing down about 10% of the internet (Newton 130). |
| Back Door | A method of accessing password protected systems without the password. May be installed during design or after successful attack (e.g., virus, worm, buffer overflow). | Provides hacker with access to computer system after attack. May not be identified even after correcting the vulnerability that enabled the initial successful attack. |
| Sniffing | Like a wiretap, for eavesdropping. A sniffing device will examine IP packets as they pass. It can be performed over a variety of mediums (e.g. copper wire, air, fiber optic cable) and equipment. | Loss of confidentiality. An attacker can potentially overhear private/confidential calls. Even if conversation is not decipherable, attackers can sometimes gain useful information by analyzing the flow of packets (i.e., where the packet came from, and where it is going.) |
| Spoofing | Impersonation. When an attacker pretends to be someone else, whether they fake their email address, IP address, or any other address. | Allows access to devices that believe the illegitimate address is authentic, or masks the origin of malicious packets to circumvent security measures. |
| Man-in-the-Middle | A situation where a hacker is able to intercept and sometimes modify packets between two endpoints. | Confidentiality and integrity of messages are at risk to this attack. |
| Address Resolution Protocol (ARP) Poisoning | ARP is used to map IP addresses to hardware addresses. "ARP Cache Poisoning" is an attack where ARP tables with mapping information are changed. | Packets may be redirected to intercept a call or eavesdrop on a conversation without the end user's knowledge. |
| Trivial File Transfer Protocol (TFTP) | A simple protocol used to transfer files. Some IP Phones automatically configure themselves from TFTP servers. | An attacker may attempt to get an IP Phone to reboot, and then spoof the TFTP server, gaining remote access to the IP Phone via a configuration file uploaded from that server. |
| Social Engineering | Someone who impersonates another person, usually over the phone, to gain special knowledge to gain access to network equipment. | Many people are fooled, providing valuable knowledge to aid attackers in gaining access to network devices, often under the name of the victim. |
| Forced System Restart | An attacker will crash a system to get it to reboot. When these systems restart, they often return to their default settings and configurations, usually with weaker security mechanisms. | An attacker will follow up with another attack to gain access to the system or device. The spoofing attacks on DHCP and TFTP describe above are examples. |
| Default/Weak Password | Many network devices are delivered with well-known default passwords. Users fail to change them or replace them with passwords that are easy to guess. | Devices with unchanged default passwords or passwords that are easy to guess with software (e.g., dictionary words), are extremely vulnerable to access by unauthorized individuals. |

Table 2. Specific Methods of Attack on Network Systems

A DoS attack can be performed simply by sending hundreds of packets per second to a network switch until it is no longer able to handle the volume. More commonly, however, malicious parties use many computers (called Zombies) in parallel to send a flood of data in a Distributed DoS (DDoS) attack. The hacker gains control of these Zombies through the use of malicious code implanted on the computer by viruses, worms, Trojan horses, buffer overflow attacks or other means (see Table 2). The Slammer Worm is a well-known example of a DDoS attack that quickly disabled an emergency 911 system in Bellevue, Washington. The call center had to track calls manually until the issue was resolved, illustrating the potential damage that a DDoS can have on essential network functions (Newton 926).

An attacker may not need to knock out network equipment to prevent telephone service, but may gain control of system devices to work against you without your knowledge. They make changes to configurations, often affecting changes in traffic flow. For instance, a person who gains unauthorized access to your IP phone could have all calls automatically forwarded to a different number and you wouldn’t know the difference. Table 2 provides examples of a variety of methods to accomplish this type of call hijacking.

Finally, the most annoying form of denial of service is caused by spamming. Just as email inboxes fill with unsolicited and unwanted messages, IP phones can be hit with numerous calls that are difficult to trace (unlike PSTN calls). Some consider this a form of denial of service for two reasons: legitimate calls are missed when filtered

out by anti-spam mechanisms and lines become tied up until the spam phone call is recognized for what it is.

### 2. Compromise of Confidentiality

Confidentiality describes the ability to keep private, confidential, or propriety information secret. Failure to maintain confidentiality can lead to such penalties as identity fraud, the loss of competitive advantage related to leaked corporate secrets, and National Security risks when sensitive information is compromised. IPT vulnerabilities provide opportunities for hackers to eavesdrop on conversations, to track signaling, to monitor billing records, and to see private information. They can easily extract information from unencrypted packets that pass through sniffing (see Table 2) devices under their control. Your packets may pass through an attackers sniffer (1) as a necessary consequence of placing calls through untrusted networks, (2) as a result of using hubs that broadcast packets to all devices they are connected to, (3) because an attacker physically attached the device to your network, (4) because the attacker gained access to one of your network devices, or (5) because the attacker configured a network device to redirect (or send copies of) the packets (e.g., via ARP Cache Poisoning described in Table 2).

When hackers are unable to determine the content of the messages on the network, they may still learn valuable information by sniffing the network through traffic flow analysis. If attackers can determine where a packet is going to and where it came from by reading header information, they may be able to make some determinations based on predictable network behavior. For instance,

several packets going to the same address from many different addresses may indicate the location of a server and give the hacker a point to focus an attack.

Hackers are not the only enemies to confidentiality. Complacent employees, usually with no malicious intent, frequently fail to keep calls private. Whether it be speaking loudly amongst a group of cubicles, failing to close a door or window, or chatting on a wireless or cell phone, people often create vulnerabilities that no amount of network security mechanisms will overcome.

### 3. Toll Fraud

Phreakers have been trying to get free phone calls from the PSTN for years and continue to pursue the same goal on IPT-based networks. Common methods of acquiring toll free calls consist of: intercepting and rerouting signaling, gaining access to network devices that record call billing, and gaining access to another individuals IP phone. These methods are similar to those used to attack the PSTN, but are much simpler to conduct due to easier access to data networks. Although phreakers can potentially drive up telephone bills, employee abuse of telephone use is likely to come at a higher cost.

### 4. Compromise of Integrity/Authentication

Integrity describes the ability to recognize if a packet has been altered (whether by mistake or intentionally). Good integrity gives us confidence that the message received is trustworthy and in its original form. Authentication is similar and provides the means to reliably identify who a message is from. One step further is non-repudiation, a mechanism that prevents a user from denying that he or she sent a message. When in place, these

tools provide a confidence that the user on the other end is known and providing accurate information.

Hackers may attempt to subvert these mechanisms in order to spread false information, to gain access to network resources under someone else's name, or to avoid security mechanisms for other attacks. If an attacker can successfully spoof (see Table 2) another address, it will likely give them access to network resources that were previously unavailable. For instance, if hackers can convince an IP Phone that it is receiving a legitimate configuration file from its server, they can reconfigure the IP Phone to suit their needs. Caller ID is an example of a telephony feature that has been successfully spoofed on IPT-based networks. Hackers have found a way to display any number they want, and can even bypass Caller ID blocking to discover the phone number of anonymous numbers (Poulsen).

### 5. IPT Components

The components of the IPT-based network are the focus of attacks, usually to disrupt service or to gain unauthorized access. Hackers will use a combination of the attacks listed in Table 2, and others, in order to meet their goals. The main elements of the IPT-based network that they will attack are the endpoints, switches, servers, and gateways.

The endpoints of the IPT-based network are typically the phones and computers where voice conversations begin. Where telephone handsets of the PSTN are usually ignored as avenues of attack, IP phones are targeted extensively as a viable point of unauthorized access. The intelligence contained in the phones allows much more control of the

network. Hackers gain access to IP Phone configurations by forcing IP phone reboots, spoofing TFTP servers, and by other methods mentioned in Table 2. Softphones are even more vulnerable because they are software programs that create virtual telephones on a computer. They become susceptible to any of the worms, viruses, or operating system/application software bugs that the computer may encounter. The hacker has access to a considerable number of tools to gain access to IPT-based network endpoints.

The switches and routers on the network are targeted to disrupt or redirect the flow of traffic on an IPT-network. A hacker will attempt to use many of the attacks already discussed to eavesdrop or intercept phone calls at switches on the network.

The servers in an IPT-based network hold most of the information of value (e.g., billing, address translation, configurations, etc.) and are thus a prime target. Hackers use many of the same attacks discussed to gain control of the servers or disrupt the network by bringing them down. "Compromising an IPT-based server usually leads to the total compromise of the IPT telephony network the telephony server is a part of" (Keneipp 15).

Gateways provide an interface between IPT-based networks and other telephony networks, like the PSTN or ISDN. The complexity of interfacing dissimilar networks provides great opportunity for hackers to identify bugs or to use known vulnerabilities of either network. They can subsequently exploit those bugs with the potential of gaining control over components of both networks, a vulnerability that was less common to the PSTN prior to the emergence of telephony over packet-switched networks.

## E. MANAGING SECURITY RISKS

The long list of IPT threats and vulnerabilities might suggest that IPT is not ready to fill the role of the PSTN. However, there are many mechanisms that are currently in use or being developed to alleviate the risks presented. Although some tradeoffs of the qualities and protections of the PSTN are required, the risks of using IPT can be mitigated to the point where the benefits of IPT will far outweigh the services of the PSTN. The next section will describe the type of security approaches required to ensure the success of IPT.

### 1. Policy

Organizations must continually create, review, and update IPT-based network security policy. IPT continues to grow and change rapidly, creating the need to frequently reassess and adapt a security strategy that balances the goals of the business with the current IPT environment. Policy must include measures that ensure compliance to the procedures set forth and adequate training and education for network administrators. One of the greatest vulnerabilities to a company’s security posture is created by those personnel who fail to properly implement security mechanisms as prescribed.

### 2. Physical Security

Physical access to all IPT equipment should be closely monitored and limited to authorized personnel only. Critical components of the IPT-based network should be kept in a locked room or datacenter. This equipment would include servers, gateways, IP PBXs, databases, routers, and network management systems. Potential methods of access control include: electronic ID cards, keys, badges, combination locks, keypad systems, biometric devices, and

human guards. Be sure to log each visit, whether electronically (e.g., with electronic access card) or handwritten log. Visitors should always be escorted. Consider the use of motion detectors and closed circuit television. Securing the space in this manner reduces avenues of unauthorized physical access and minimizes accidents by reducing unnecessary traffic.

Equipment in the secured space can further be protected by using installed locks and keeping special knowledge out of view (e.g., passwords and configuration settings). Less critical equipment that is not located in the datacenter, like cabling and switches, should be kept behind locked doors and run behind walls and ceilings. All unused ports of any equipment should be disabled.

Finally, preserve network equipment by controlling the environment and planning for natural occurrences. Equipment should be stored in rooms with good ventilation to prevent overheating and air conditioning to reduce moisture in the air. Prepare for power outages by installing uninterruptible power supplies or backup generators. Develop disaster recovery plans, pay for insurance, and build in redundancy to minimize losses from physical damages caused by acts of nature.

### 3. Logical Separation

Once the network is physically protected, it is necessary to design a network topology that will provide the best security. It is possible to create another physical network specifically for IPT to significantly reduce the risks of vulnerabilities and performance reductions introduced by the data network. Although it provides excellent security, it is not a desirable

implementation because it is costly to install, maintain, and manage the extra cabling and equipment. Additionally, it would eliminate the benefits gained by converged data and voice networks. To both minimize vulnerability and increase efficiency, the IPT-based network should be logically segregated from the data network. This can be accomplished by putting IPT components on a separate VLAN (see Table 3), by using switches in preference to hubs, and by using a private IP address space (see Table 3).

| Security Mechanism | Description |
|---|---|
| Virtual Local Area Network (VLAN) | A VLAN is a logical (virtual) grouping of network devices regardless of their physical location on the network. A VLAN allows more efficient traffic routing and segmentation of similar system applications to minimize security risks. For instance, VLANs may be used to segment network equipment among one company department, wireless equipment, IPT phones, or IPT servers. |
| Private IP Address Space | IP address ranges specifically dedicated for internal use in an organization's network. These addresses are not valid (i.e. you can't route traffic) external to the network. The ranges are: 10.0.0.0 through 10.255.255.255, 172.16.0.0 through 172.16.255.255, and 192.168.0.0 through 192.168.255.255. |
| Firewall | A firewall is a system implemented in a combination of hardware and software that enforces a boundary between two or more networks. Packets entering or leaving the network are examined, then let through or blocked according to specific criteria. These criteria are determined according to security policy intended to limit potential avenues of attack. Firewalls filter with different granularity, examining basic address information up to application level information. Simple firewalls are typically faster and less expensive because they inspect less information; while, firewalls that examine deeper into packets become more expensive, especially if faster processing is required. A firewall is analogous to a security gate at a secured facility. All traffic in and out of the facility must pass through the gate and will be inspected according to established policy. Anything entering (e.g., person without identification) or leaving (e.g., government property) that violates policy will be blocked. |
| Stateful Firewall | There are two types of packet filtering firewalls, stateless and stateful. A stateless firewall has no memory of traffic it has processed. A stateful firewall remembers previous traffic and can adjust filtering decision dynamically to allow certain connections. For instance, when a user sends a packet to an address outside of the network, the firewall will remember the external address and allow those packets inbound if addressed to the internal user. |
| Intrusion Detection System (IDS) | An IDS is a program that monitors network traffic or system processes and analyzes them for malicious attacks. Sometimes the IDS will send an alarm, while other times it may block the data flow. An IDS must be tuned to find the right balance between false positives (blocking legitimate traffic) and false negatives (allowing malicious traffic to pass.) There are two types of IDSs, Network IDSs (NIDS) and Host-based IDSs. NIDS monitor packets on the network, usually at the perimeter. HIDS are installed on individual machines and work to detect attacks originating within that specific computer. |

Table 3. IPT Security Mechanisms

The logical separation of the two networks promotes better IPT performance, because IPT components can ignore traffic generated by data protocols and applications, and

give priority to specific IPT traffic. The reduced interaction between voice and data improves security by minimizing, but not eliminating, exposure to attacks (e.g., worms, viruses, DoS) on the data network. It should be noted that softphones actually lie on the data network and should be segmented to avoid exposure to these attacks as well. The segregation of the two networks also achieves better resistance to eavesdropping attacks. To achieve the full benefits of segregating the voice and data networks, switches (more expensive) must be used rather than hubs (i.e., no VLAN at hubs).

The IPT-based network may be isolated further by using a private address space, facilitated by NAT. It can serve two purposes: first, to disguise the location of IPT components from external devices, and second, to share the use of external IP addresses among several devices. Unfortunately, these benefits are offset by the complexity of using NAT with IPT. NAT traversal mechanisms must be considered and in place to take advantage of the private addresses and to assure reliable IPT telephone sessions.

**4. Manage Network Traffic**

Firewalls, Intrusion Detection Systems (IDS)(see Table 3), and NAT traversal mechanisms are measures used at network boundaries to provide protection from external threats. Careful planning is required to ensure these devices are deployed in the right places with functionality appropriate to the needs of the network. Network managers must understand what they are willing to pay to achieve both performance and security.

Firewalls are essential network security tools that are used to block undesirable traffic, both entering and

leaving the network. However, they form bottlenecks that add delay to the system, significantly impacting the quality of IPT communications. This is enhanced by the fact that IPT firewalls must be stateful (see Table 3) to recognize IPT packets that would otherwise be blocked. These delays are mitigated by segmenting networks and by using firewalls designed for use with IPT-based networks (i.e., they are stateful and recognize SIP and H.323 protocols), but come at a significant cost to achieve efficiency.

Network IDSs (NIDS) are generally placed in the same portion of the network as firewalls where they can observe traffic that flows in and out of the data network. A NIDS examines packets (without adding significant delay) to detect malicious attack traffic and warn system administrators. Some have the ability to block the traffic, but are generally used to observe. NIDS must be carefully tuned to avoid either blocking legitimate traffic or allowing malicious packets.

NAT is not so much a security mechanism, as it is a method to map private addresses to externally routable IP addresses. The use of NAT must be carefully planned for and considered with IPT-based networks, however, because it is difficult to establish and maintain IPT connections without the proper systems in place. Table 4 provides a general description of NAT and the current methods used to negotiate it. No single method of NAT traversal is ideal for all network environments, especially since the problem is relatively new and solutions are slowly evolving. Each mechanism has its advantages and limitations and must be evaluated in the context of the specific IPT-based network.

Recently, the use of STUN, TURN, and ICE protocols appear to be the most promising.

| Mechanism | Description |
|---|---|
| Network Address Translation (NAT) | NAT can be implemented in a variety of ways to map private addresses in an internal network to a set of valid external IP addresses at the network perimeter. It has the advantage of sharing a limited number of valid external IP addresses among many internal devices and of virtually hiding the internal devices from external users. The disadvantage of NAT is that translation can become very complex, particularly for incoming traffic, and causes complications with the use of firewalls and VPNs. This means that very expensive solutions are required to make IPT phone calls without significant delays or dropped calls. |
| Application Layer Gateway (ALG) | This is a stateful firewall that can be used specifically for IPT-based networks. It is able to understand packet information pertaining to SIP or H.323 call control, and make appropriate filtering decisions to accommodate most IPT voice traffic through NAT. Unfortunately, an ALG can introduce latency, jitter, and network congestion into the system during times of high call volume and is often expensive maintain. They are also known to interfere with secure SIP signaling and STUN. |
| Middlebox | A Firewall Control Proxy (FCP) is an example of a middlebox device that is intended to improve the performance of firewalls (like ALGs) that filter IPT traffic. The FCP inspects IPT traffic and tells the firewall what traffic to allow, significantly improving throughput. The weakness of a FCP is that it becomes another point of attack that must be protected. If an attacker gains control of an FCP, the firewall will be compromised as well because it completely “trusts” the FCP. |
| Simple Traversal of UDP through NAT (STUN) | STUN is a protocol that allows IPT applications and devices to identify NATs and firewalls in a communication path between two endpoints. This helps to facilitate call setup and reliable channels of communication that pass through NAT devices. STUN is not effective for all NAT implementations or telephony connections (e.g., TCP). |
| Traversal Using Relay NAT (TURN) | TURN is a protocol intended to overcome the limitations of STUN. TURN is more complex and comes at a cost of reduced scalability and performance. |
| Interactive Connectivity Establishment (ICE) | ICE is a methodology used with the same goals as STUN and TURN, that is, to allow reliable channels of communication through all forms of NAT devices. ICE uses existing protocols to determine which method of NAT traversal (i.e., STUN or TURN) will provide the best connection for an IPT call session between two endpoints. |

Table 4. NAT Traversal Mechanisms

### 5. Harden IPT Equipment

IPT-based network equipment must be secured to prevent hackers from gaining control of critical network devices. Call servers, mail servers, and other IPT-based network servers hold sensitive data and perform critical functions that require special defenses. Servers should be hardened by doing the following:

- Install the operating system on a clean hard drive.

- Apply all the latest patches. Patches contain fixes to newly discovered vulnerabilities. Subscribe to a service that will provide continuous updates on new patches.

- Run a vulnerability assessment tool. These tools allow network managers (or hackers) to scan network equipment for known security holes. After discovering the vulnerabilities, either take the steps necessary to correct them or accept the risk that they represent.

- Install a firewall on the server computer. Start with a restrictive policy (don’t allow any traffic) and then open only those ports required to serve its function.

- Consider installing a host-based IDS.

- Install antivirus software and ensure it is up to date. Antivirus software is designed to scan files for viruses, worms, and Trojan horses. Most are signature-based, looking for lines of code distinct to particular viruses. Signature files are updated frequently to protect from the newest, known viruses. Utilize automatic update functionality that will automatically check for updates and download them.

- Create an image after following the steps above and use it to create other IPT servers.

- Change default configurations to match security policy. This can be done using software. Adjust the boot sequence to prevent hackers from gaining access by forcing a system crash and reboot. Be sure default passwords are changed.

- Turn off or disable all unnecessary services and applications that are not in use. This may include disk drives and physical ports. Each service is a potential avenue of attack for a hacker.

- Avoid the use of shared drives.

Hardening these servers causes little delay and helps to protect against the bulk of external attacks on these IPT components. Combined with good physical protection and logical separation from the data network, these systems can help establish relatively secure IPT sessions.

Other IPT equipment must be hardened in a similar fashion. IP phones, for instance, have several vulnerabilities in a default state. Passwords must be updated and authentication required, all unnecessary services must be disabled, and reboot sequences must be updated to prevent unauthorized access to the equipment. Automatic registration is often used to install many IP Phones at once, but should be disabled immediately to prevent an attacker from restarting the phone and gaining access by spoofing the registration server. Treat public IP Phones differently by limiting available features and services.

Softphones also require special hardening since they reside in a portion of the data network on computers. They must have the latest patches and antivirus software to be protected against worms, viruses, Trojan horses, and buffer overflow attacks. Unnecessary services must be restored. Because they are more closely tied to the data network, softphones are more likely to be affected by attacks and suffer from reduced voice quality. All other network

components should receive the same kind of attention to secure the network from known attacks.

### 6. Encrypt and Authenticate IPT Traffic

Encryption is required to establish confidentiality (i.e., prevent eavesdropping) both within the network and through external networks. A Virtual Private Network (VPN) incorporates end-to-end encryption to “tunnel” through untrusted networks. This allows IPT traffic to flow securely from an organization’s intranet and through internets, that aren’t trusted, to the other end. It also allows employees to connect to the company’s intranet from an external source and provides a certain level of authentication. Table 5 provides a few of the common mechanisms used to keep voice conversations private, including the favored protocol IPsec.

| Security Mechanism | Description |
|---|---|
| Virtual Private Network (VPN) | “A VPN is a ‘virtual’ network that is kept private by ‘tunneling’ private data through the underlying infrastructure of the public Internet” (Mairs 208). Tunneling basically allows the connection of two networks that are separated by an untrusted medium. It ensures the security of data flow by using end-to-end encryption and encapsulation. First a data packet is encrypted at the endpoint, that is, the data is scrambled into an unreadable format that may only be unscrambled by a trustworthy user at the other end. Then the encrypted data is enclosed (called encapsulation) in the packet of another protocol and sent across the appropriate network. When it reaches the other end, the protocol headers are removed and the data is deciphered. This method of data protection improves security, but creates delay to perform encryption and encapsulation. |
| Internet Protocol Security (IPsec) | “IPsec is the preferred from of VPN tunneling across the Internet” (Kuhn 63). IPsec has two basic protocols: Encapsulating Security Payload (ESP) and Authentication Header (AH). ESP primarily focuses on ensuring data confidentiality and some authentication, while AH provides authentication and integrity. Since ESP creates more delay to ensure privacy, AH can be used only where authentication is necessary. IPsec also has two delivery modes: Transport and Tunnel. The modes are similar, but tunnel mode encrypts more packet information to minimize traffic flow analysis and provide better security. This comes at a cost of increased delay. |
| Secure Real-time Transport Protocol (SRTP) | “SRTP provides a framework for encryption and message authentication of RTP and RTCP streams. SRTP can achieve high throughput and low packet expansion” (Kuhn 69). SRTP provides a method to protect the confidentiality of voice conversations without adding significant overhead and delays to RTP packets. |

Table 5. Encryption and Authentication Mechanisms

The major disadvantage of encryption is that the process of scrambling and unscrambling information can add

substantial delay. This significantly impacts the voice quality of a real-time application like IPT. Organizations have been able to effectively apply encryption to IPT conversations, but it requires a careful initial assessment of network capabilities and subsequent investment in upgraded equipment. After that, consistent performance can be achieved by continued evaluation (and tweaking) of network performance using network management tools.

### 7. Redundancy

In order to approach the reliability of the PSTN, an IPT-based network must take a similar approach to redundancy. A focus on several areas of redundant systems will improve the chance of quick recovery when disaster strikes. First, the data must be protected by making regular backups of critical systems. They should be created in reliable memory systems and stored in a secured, offsite location. Second, the network is protected using a layered strategy or “Defense in Depth.” This describes the use of several security mechanisms that complement each other and overlap, rather than a reliance on a single defense. Third, the operation of critical equipment is assured by providing redundant systems that are ready to go online when the current systems fail. All equipment is protected from power fluctuations and power loss with surge protectors and Uninterruptable Power Sources to allow controlled shutdowns. Critical systems are backed up with generator power. Fourth, the IPT-based network is supported by out-of-band communications, usually the PSTN. PSTN will still be around for awhile. Organizations should feel comfortable with a telephony architecture that utilizes the benefits of both the PSTN and IPT to meet its needs. Finally, Disaster Recovery Planning (and practice) must be a regular part of

every organization’s network policy. Even if disaster never strikes, effective use of this type of planning will help businesses learn to identify potential risks and losses and the costs associated with them. The ability to effectively balance the cost of risk mitigation strategies with the cost of actual losses will provide those companies with a competitive advantage.

#### 8. Weighing the Costs

The security measures described offer methods to protect against the vulnerabilities of computing systems and packet-switched networks. They provide solutions to mitigate security risks to IPT-based networks, but usually at an economic cost or at a cost to call quality. Although security and voice quality often conflict, they can both rise if you are willing to pay for it. Since each organization’s security and business needs differ, they must be determined to understand their requirements and decide if they have the means to get there. Recently, it appears that more and more businesses have come to the conclusion that they can afford to secure an IPT-based network and enjoy the benefits it provides.

### F. SECURITY POLICY AND GUIDANCE REVIEW

Now that the management of IPT security risks has been discussed, it is appropriate to examine how to enforce effective security practices with good security policy and guidance. The next section will briefly define what good security policy is and describe how to create it. Then, a variety of current information technology policy and guidance will be reviewed. Policy from the Coast Guard and other government agencies will be examined to understand how each policy is relevant to IPT and how it might be used to create Coast Guard specific policy. The combination of

information gathered from these policies, other research, and a study of a Coast Guard’s implementation of IPT were pulled together to make recommendations for IPT Security Policy in the Coast Guard. These recommendations are presented in Appendix A.

### 1. Creating Effective Policy

Policy consists of an organization’s guiding principles and mandates that express management’s goals and objectives about a general issue. It should be brief, concise, clear, stable, and written in the active voice. A good security policy will (1) address the level of risk that management is willing to accept, (2) specify who is responsible for what actions and how they will be held accountable, (3) identify how results are to be measured and reported, (4) and be expressed in terms that are appropriate to the specific system being discussed in the context of its role in the organization (Murray Notes). Good security policy is created by adhering to these guidelines and by considering Courtney’s Laws (i.e., three laws created by Robert H. Courtney, Jr.):

> (1) Nothing useful can be said about the security of a mechanism except in the context of a specific application and environment.
>
> (2) Never spend more mitigating a risk than tolerating it will cost you.
>
> (3) There are management solutions to technical problems, but no technical solutions to management problems (Murray Notes).

The objectives of a security policy are enforced through the use of standards, guidelines and procedures.

Standards are more specific than policy, providing measurable rules and regulations that support the policy and are required. Guidelines are usually suggested (i.e., optional) techniques to understand how to meet standards and policies. Procedures are even more specific and describe how to meet standards well, by providing step-by-step methods. As you move from one end of the spectrum at policy, where intent is broadly defined and relatively unchanging, to the other end at procedures (via standards and guidelines), objectives become more specific and more volatile to meet the needs of the current technology (Murray Notes).

In this document, policy generally refers to documents that describe an organization’s overall approach to dealing with information technology security and the types of standards that are mandated, while guidance typically refers to documents that describe methods (i.e., guidelines and procedures) to implement policy and standards. However, policy may sometimes include options and guidance may include requirements.

## 2. Coast Guard Policy Review

The documents described in this section mandate the use of information technology in the Coast Guard. They have been studied to determine how they are relevant to IPT and what type of standards and guidance they have not addressed. The information gleaned from this analysis is presented below and has been used to develop specific IPT Security Policy and Guidance in Appendices A and B.

### *a. COMDTINST 5230.56: Policy on Coast Guard use of Internet/Worldwide Web*

The purpose of this policy is to regulate “Internet site management, page content, page development,

and usage” (1). It applies to all Coast Guard units that use the WWW to share or access information, whether it is on the Coast Guard Data Network (CGDN) or other networks. It provides direction and guidance, to commanding officers and information technology staff, on what type of information may be shared on the WWW and how it must be protected. The security issues briefly addressed cover the protection of web site information and equipment. It does not directly address IPT, but can be referenced to appropriately manage the configuration of IPT equipment via web browsers.

#### ***b. COMDTINST 5375.1A: Limited Personal Use of Government Office Equipment***

This instruction defines the policy for the personal use of government office equipment, which includes information technology equipment, by all Coast guard personnel. It sets restrictions on the appropriate times and duration that office equipment may be used for non-work activities. It also specifically prohibits certain activities and sets forth disciplinary measures for failure to meet standards.

Although, the policy does not specifically mention IPT (nor does it address security), the use of IP Phones and other IPT equipment easily falls under the standards set for telephones and other information technology equipment. The most relevant standards include limits on personal telephone calls, prohibitions on downloading personal software and connecting personal hardware, and restrictions on the content (e.g., illegal, offensive, personal business, confidential, etc.) of information. IPT specific policy and guidance can refer to this policy for appropriate use of IPT-based systems.

### *c. COMDTINST M5530.1C: Physical Security and Force Protection Program*

This program sets forth policy, standards, guidance, and procedures to assure the physical security of a variety of Coast Guard resources, including: facilities, computers and networks, firearms, ammunition, explosives, personal electronic devices (PED), telephones and switches, funds, vehicles, property, and medical substances. It describes the use of many measures to use to provide for the physical protection of these resources from basic physical barriers to human security forces. It also addresses antiterrorism policy and the response to bomb threats and other incidents.

The Coast Guard Physical Security and Force Protection Program is an important tool to determine how to physically protect IPT equipment. It provides specific guidance on how network equipment should be protected based on one of three categories: Classified Information Systems (CIS), Sensitive/Critical Information System (SCIS), Non-Critical Information System (NIS). Depending on the particular IPT application, different levels of physical security must be applied as prescribed in the program. The program also describes how to protect PEDs, telephones and telephone switches, primarily to ensure private exchange of information. The same physical security measures must be applied to IPT-based equipment that fall within these categories (e.g., wireless telephones, IPT Phones, servers) to ensure confidentiality. IPT specific guidance can refer to this program to address most IPT physical security issues.

#### d. *COMDTINST M5500.13B: Information Assurance Manual*

The Coast Guard Information Assurance (IA) Manual sets forth the responsibilities of carrying out the IA Program which…

> provides a baseline of IT security policies, standards, and guidance. The IA program outlines policies that relate to management, operational, and technical controls that provide the foundation to information confidentiality, integrity, availability, authenticity, and nonrepudiation within the CG's information infrastructure and operating environment (1-1).

The manual does exactly what it says in a manner consistent with the characteristics of good policy described above. It provides a strong foundation for data network security practices to be used by Coast Guard information technology professionals.

This document briefly mentions the use of IPT, touching on redundancy, identification and authentication, audit logging, integrity controls, and physical security. However, this program does not adequately address security issues unique to IPT-based networks. IPT-based security policy can refer to this program for many aspects of sound network security principles, but must rely on other sources for IPT-specific concerns.

### 3. Other Government Agency IPT Policy and Guidance Review

The documents described in this section provide guidelines that are not required by the Coast Guard, but may provide insight into IPT security relevant to the Coast Guard environment. They have been studied to determine how they address current IPT-based network implementations and security issues. The information gathered from this

analysis is presented below and has been used to develop specific IPT Security Policy and Guidance in Appendices A and B.

### *a. Defense Information Systems Agency (DISA) Voice Over Internet Protocol (VOIP) Security Technical Implementation Guide*

The DISA VOIP Security Technical Implementation Guide provides specific guidance on the use of IPT to units in the Department of Defense (DoD) that choose to employ IPT. It is intended to be "a tool to assist in securing…DoD networks and systems supporting" IPT technology (7). The document provides a brief overview of IPT and addresses many IPT security issues, most of which have been discussed in this chapter. Security risks are resolved or mitigated through the use of both mandatory standards and suggested guidelines. The Coast Guard is not required to follow this guidance, but may use the information provided as a strong outline for Coast Guard specific IPT security policy.

### *b. Special Publication 800-58: Security Considerations for Voice Over IP Systems: Recommendations of the National Institute of Standards and Technology (NIST)*

NIST has prepared this document as a guideline for federal agencies to use and adapt to meet their specific IPT security and business requirements. It is designed to provide guidance to establish secure IPT networks, with a focus on overcoming complications (e.g., reduced voice quality, NAT traversal) introduced by security requirements of IPT (10, 13). The document includes discussions on IPT basics, performance and quality, protocols, firewalls, address translation, call setup, encryption, IPsec, and others. NIST summarizes its findings with nine recommendations to implement a secure

IPT network. The information in this document provides current information on IPT-related security issues and can be used extensively to derive Coast Guard specific policy and guidance.

THIS PAGE INTENTIONALLY LEFT BLANK

# IV. IPT IMPLEMENTATION PRACTICES

## A. PURPOSE

Despite the continuous change occurring in the area of IPT, the technology has been in use long enough to develop practices that yield successful IPT deployments. However, there is not a “one size fits all” approach that is appropriate for all organizations. IPT implementers must carefully analyze their current network architecture and pursue IPT solutions that can best be adapted to their agency. This chapter contains a list of the attributes of successful deployments and the methodologies used by thriving businesses that have exploited IPT systems to gain a competitive advantage.

## B. IPT NETWORK CHARACTERISTICS

Burton Group has cataloged several areas of focus that must be considered to realize viable communications using packet-switched networks (*IP Telephony* 6-13 and *Voice over IP Architecture Workshop* 4-6). Proactively addressing each of these technical and operational issues is a common success factor among organizations that have already attained the benefits of IPT.

- **Cost**: The costs of IPT already discussed present a solid argument for a transition away from the POTS; however, an IPT-based network may not be the best solution in all cases. It is unwise to invest in technology just for technology’s sake. Each organization must carefully consider its options and make an unbiased business case for a particular telephony implementation.

- **Security**: As discussed in depth, each company must plan for security up front and determine the level of

risk it is willing to accept. They must be willing to pay for a level of security that is comparable to that which the PSTN currently provides.

- **Sound Quality**: Sound quality and security are often at odds with each other in an IPT-based network. It is very difficult (i.e., expensive) to realize high levels of both quality and security equal to that provided by the PSTN. A business must understand its regular (and worst case) telephone usage to determine the resources consumed by good quality phone calls. It must them provide the required mechanisms (e.g., bandwidth, prioritization (sometimes referred to as quality of service), IPT specific network equipment, etc) to meet the need.

- **Resiliency**: The availability of a telephony system is critical to any organization's success. An IPT-based network must provide a variety of backups to meet this requirement, including redundant: power, memory, systems, applications, network components, and communications (e.g., PSTN line).

- **Power and Reach**: Many phones are located in places where there is no need for computers, so there is not any power or network wiring in place. Sometimes these points are extended using wireless devices. Companies must be prepared to provide for these cases, and understand the potential reductions in voice quality to create solutions.

- **Network Management**: IPT-based networks are not managed in the same manner as the data network. Data network personnel and telephony personnel will have to work together and learn new skills to properly manage the IPT network. The network will require constant attention to

assure quality and availability. The support of the network should be facilitated by network management tools that are specifically attuned to the needs of IPT.

- **Platform Independence/Support of Legacy Services**: A successful IPT implementation will facilitate interoperability among telephony components and be flexible to adapt to changes in the technology. Few telephony networks are solely devoted to IPT technology, but rather integrate a variety of networks to provide a competitive telephony solution. It requires careful planning to connect the IPT network to other networks, like the PSTN or an ISDN, and to connect a variety of equipment from multiple vendors. Successful businesses avoid propriety equipment and protocols, and strive for standards that bring a diverse set of elements together to form a reliable telephone system.

- **Scalability**: Just like typical PSTN PBX solutions, an IPT-based network must be flexible enough to grow and change with the organization.

- **Features**: The primary business advantage that is beginning to emerge from IPT is the diverse set of features that it promises to provide. To maximize the benefit of an IPT implementation, organizations must create IPT solutions that enable feature sets that optimize current business practices and understand how those features differ from current PSTN offerings.

- **User Mobility**: One of the advantages of IPT is the mobility that it provides to employees. This mobility can be manifest in a user’s ability to quickly change desks, change phones, or even work out of the office at

home or on the road. This is an example of the type of features enabled by IPT that must be fully understood, because they require additional security and quality of service measures to appropriately implement.

- **Emergency Services**: Emergency 911 location services are a standard part of the PSTN that many people take for granted. These services require special measures (especially because of the increased mobility mentioned above) to ensure the same level of reliability that the PSTN already provides. Each organization must ensure appropriate systems are in place.

## C. IMPLEMENTATION PRACTICES

The following section enumerates and explains a variety of practices that organizations are using to successfully implement IPT and address the issues discussed in the previous section. The methods described below are not necessarily conducted in the order listed. Some may be performed simultaneously, while other groups of processes may require multiple iterations to design the right IPT solution. The practices discussed should be adapted to meet the needs of a company within the context of its environment. A manager's guide has been developed to facilitate Coast Guard IPT implementation and is included in Appendix B.

### 1. Form an Implementation Team

Since IPT brings together the data network and the telephone network, personnel with training and experience from both backgrounds are required to understand the new system. An organization must form a team that taps the resources of employees with varying specialties (e.g., telephony specialist, network manager, security

professional, finance, legal, etc.) so that all issues may be addressed. The team members must receive the training and develop the experience necessary to interface ideas and processes. The collaborative process must not only include the exchange and fusion of information, but must also share sources of power (e.g., budget, resources, management support, etc.). Each member should expect to have a different understanding of the data and telephony networks, and how they support business objectives, when the implementation is complete.

The IPT implementation team may be supported by personnel, called system integrators, who are brought in from outside of the company to help design an IPT solution. Outsourcing pieces of the implementation has the advantage of providing in depth knowledge and experience about IPT. This know-how usually comes more quickly and at a lower cost than if the company was to train its own IPT experts. According to a survey conducted by Integrated Research, approximately 34% of companies use or plan to use system integrators for their IPT deployments (Integrated Research 6).

When selecting system integrators, an organization should review and weigh the integrators' level of quality, expertise, capability, integrity and cost. The organization must also establish service-level agreements. The contract made with the system integrator should include training and support so that the system is properly maintained when the system integrator leaves (Walker 130-134).

**2. Understand Current Telephony Requirements**

Before replacing components of the POTS with IP Telephony, an organization must first understand its

current telephone usage. Fortunately, the PSTN has a well established system of capturing characteristics of telephone calls made over the network. Call Detail Records (you’ve seen these in your monthly itemized long-distance bill) are an example of records that track calls. The IPT deployment team should locate call records and determine the telephony requirements of the organization. Statistics of interest include: number of calls, number of users with distinct phone numbers, duration of calls, number of concurrent calls, source and destination of calls (within site, within business, external, international versus domestic), and call volumes. Call volume profiles are especially important for determining network capacity. Call volume peaks and averages should be discovered with an understanding of when peaks occur, for how long, and if they cause (a percentage of) blocked calls. Understanding these requirements will facilitate the development of an IPT-based network design that accommodates the organization’s needs (Walker 64-66).

While reviewing call records, it is a good time to review telephony costs and carrier contracts. Identifying these costs helps to justify the IPT implementation, but may also point out potential areas of increased costs. For instance, most businesses incrementally deploy IPT and continue to rely on existing PSTN services. An organization that deploys IPT may reduce the number of calls on the PSTN, but actually cause an increase in telephony costs. This can happen when the reduced PSTN call volume falls below a threshold where “bulk” rates are applied. Even though there are fewer calls, those calls become more expensive and may actually drive up costs.

Finally, the IPT project team must work to understand user requirements and expectations. It is commonly accepted that the PSTN provides “five nines” of availability and toll quality calls. Users have come to expect that level of performance along with the other features they already use. Current capabilities must be cataloged and prioritized so that they can be enabled in the IPT-based network. Examples of some of these requirements include: voice mail, conferencing, customer relationship management tools (a.k.a. phone trees), simple phone interfaces, simple dialing plans (how many extra numbers does the user need to dial to get an outside line balanced with how few to dial internal extensions), features mentioned in Chapter I, and others. User expectations must be managed if those capabilities are going to be reduced in trade of other improvements or lower costs.

### 3. Understand the Data Network Infrastructure

To converge voice and data, we must understand both the PSTN and the data network prior to deployment. Many believe that IPT can just be thrown on top of the data network like any other application, but soon discover that IPT has special requirements that necessitate adjustments to the network and require more stringent monitoring.

> The technology that is currently available from mainstream vendors is ready for enterprise deployment but many problems still occur, primarily from insufficient network preparation (Integrated Research 5).

Adequate network preparation begins by identifying the current characteristics of the data network so that adjustments can be made to support IPT. This type of

evaluation must be performed at three levels as appropriate to the implementation: (1) over the local area network, (2) over the enterprise wide area network, and (3) over the Internet (although the ability to make changes will be limited). Most IPT professionals agree that some sort of data network audit or assessment for any implementation is vital to successfully deploy IPT. John Walker and Jeffrey Hicks explain such a process in “Taking Charge of Your VoIP Project.” Their methodology is described below.

- **Configuration Assessment**: The purpose of this assessment is to examine network equipment to determine what must be upgraded to handle IPT. First, all network equipment must be identified and inventoried. The equipment characteristics that should be checked include: the operating system version, the amount of memory, the existence and types of Quality of Service mechanisms, presence of VLANs (data, voice, and wireless should be separate), presence of hubs (should be removed), interface speeds, and how power is supplied to the phone. Then each piece of equipment must be compared to a set of criteria to determine if it will support IPT traffic, functionality, capacity, reliability and call-quality (93-95).

For example, a configuration assessment might reveal that a network router has an interface speed of 100 megabits per second (Mbps). Based on peak call volumes, the speed will not be able to handle all calls without degraded call quality or dropped calls. The router must be upgraded (e.g., 1000 Mbps) to support the new IPT-based network.

- **Utilization Assessment**: The purpose of this assessment is to identify to what degree network devices and links are being utilized. Average values, peak values,

and times of high utilization are important metrics to observe. Utilization rates that approach 100% suggest problem areas for IPT implementation, which must be managed or corrected via equipment upgrades. The following dimensions should be measured to ensure the support of IPT traffic, functionality, capacity, reliability and call-quality: CPU utilization (device’s workload), memory utilization (e.g., size of jitter buffer), backplane utilization (amount of traffic moving through switches), dropped packets (occur at bottlenecks), buffer errors (usually indicates inadequate memory), interface errors (usually indicate problems with physical transport medium), and bandwidth utilization (the percentage of bandwidth being used). Bandwidth utilization is a good indicator of network capacity and should always be closely monitored, particularly on wide area network links where delays are more likely. (95-97).

- **Call-Quality Assessment**: The purpose of this assessment is to determine how well the network would support good call quality by simulating IPT traffic and measuring the flow of information for delay, jitter and packet loss. These measurements are used to estimate a mean opinion score to determine call quality.

The following characteristics of IPT equipment and packets will affect the flow of information: The type of codec used (the compression algorithms and data rates it uses, and the packet size it produces), voice packet sizes (smaller packets move more quickly but have more overhead), the use of Voice Activity Detection, the size of jitter buffers, and Quality of Service mechanisms.

The simulation allows experimentation among changes in network characteristics and is usually conducted on selected portions of the network that mostly represent the entire IPT network. From this assessment, predictions can be made about the feasibility of good call quality in an IPT implementation. It is also useful for identifying potential risks and weak points in the network prior to deployment, allowing for equipment upgrades or network configurations that will enhance call quality (97-99).

- **Bandwidth Modeling**: The purpose of this assessment is to make predictions about the actual performance of the current network with the load of IPT traffic. This process is very similar to the call quality assessment described above, but is more complex and requires many mathematical calculations to complete; therefore, it is usually conducted on critical network links first and expanded as resources permit. Bandwidth modeling allows the IPT design team to determine how well the capacity of the network handles the additional traffic introduced by IPT, based on changes in call volumes, codecs, bandwidth, packet sizes, Quality of Service mechanisms, and voice suppression mechanisms. (99-100)

**4. Update the Data Network**

After successfully auditing the data network, most organizations discover that many changes are required to adequately support IPT. According to Mack Leathurby of Avaya "…about five percent of our customers don't have to do something to upgrade their existing network" (Joch). Network changes usually focus on call quality improvements or replacing equipment to meet other requirements like security or redundancy.

Increased call quality can be achieved by cleaning up network traffic, increasing bandwidth, upgrading equipment, changing the network design, and implementing or tuning Quality of Service (QoS) mechanisms.

- **Network Traffic**: Approximately 20%-50% of network traffic is considered unnecessary, supporting unneeded services that are operating by default, usually without anyone's knowledge (Walker 104). Use a network protocol analyzer (e.g., Ethereal, EtherPeek) to identify these. Turning them off will increase bandwidth, and reduce the load on processors and memory.

- **Bandwidth**: There are several methods available that help to conserve bandwidth, some of which include: RTP header compression (cRTP), VAD, RTP multiplexing, and Call admission control. cRTP compresses RTP headers to reduce bandwidth consumption, but comes at the expense of increased handling delay. VAD reduces bandwidth consumption by sending smaller packets during silence, but can reduce voice quality. RTP multiplexing sends several voice conversations in the same packet to cut out bandwidth that is consumed by headers, but can add to delay and cause greater impact when packets are lost. Call admission control is used to limit the number of concurrent IPT calls on the network, routing extra calls to the PSTN. The benefits and disadvantages of each of these methods must be balanced to meet the requirements of the network configuration. If these mechanisms aren't sufficient to free up adequate bandwidth it may be appropriate to pay for more; however, it is important to understand the network in order to increase the bandwidth in the bottlenecks where it is needed the most.

- **Equipment**: Common equipment upgrades to improve voice quality include: Replacing hubs with switches, upgrading to more modern switches and routers that process information more quickly, increasing router memory, and preferring hardware-based firewalls to software-based equipment. These equipment upgrades help increase the processing speed of the network, enabling better call quality.

- **Network Design**: Re-engineering the network can help to improve call quality in many ways. Examine traffic flow to determine what kinds of routes are used and how many hops are required to get from one endpoint to another. Direct, shorter routes and fewer hops will help to reduce propagation and handling delays. Locate bottlenecks and points of congestion and work to eliminate them, route around them, or give precedence to IPT traffic. Finally, push processing work out to the endpoints to facilitate the movement of packets through the core of the network. This, however, requires more processing power at the edges of the network.

- **QoS Mechanisms**: As previously discussed, QoS mechanisms give priority to time-sensitive applications like IPT. They help to maintain good call quality during occasional periods of congestion.

Other components of the network must be updated to meet the needs of requirements other than call quality, like security and redundancy. These improvements are usually completed through the replacement or update of existing equipment. When updating network equipment (or when making call quality improvements), it is important to

make changes in a methodical way. First, the project team must determine which changes are the most cost effective and most important. Then, they should make incremental changes beginning with the highest priorities. After making a change, small tests and assessments should be conducting to ensure that the adjustment had the desired effect. Those that try to make too many modifications at once find that it is too difficult to identify new problems created by the change. The incremental approach also makes it easier to adjust priorities and determine when network improvements have reached an acceptable level (Walker 103-109).

### 5. Develop the Business Case & Acquire

Justifying the installation of an IPT-based network occurs prior to and throughout the implementation process. The planning and preparation phases discussed to this point help to strengthen a case to deploy IPT (or not to deploy it) by determining the organization’s requirements and by assessing the condition of its data network. These considerations must be weighed with an analysis of the costs required to go forward with a large scale implementation. This section begins by covering some common forms of IPT deployment that are known to provide good returns on investment. It follows with recommendations on the type of equipment, service, and support that the IPT project team should demand to ensure long term success. A project team that is able to demonstrate measurable benefits and the viability of IPT early and continuously will get internal commitment and budgetary support that will sustain the duration of the implementation.

IPT-based networks are rarely deployed by completely replacing old PSTN equipment with new IPT gear. The

benefits of IPT are usually realized through incremental upgrades that take advantage of the features of both IPT and the PSTN. Walker and Hicks make several recommendations, which follow, for the type of upgrades that promise large returns from minor investments for most organizations.

- **New Sites**: Organizations that are expanding to new sites can find great benefit from building new telephony service from the ground up without having to worry about upgrading an old network. With proper planning, the new office can provide dependable IPT service with room for future growth.

- **Data Network Upgrades**: If the data network already needs an improvement, the business can benefit by including IPT requirements in the planning requirements.

- **Excess Capacity**: Bandwidth and processing power have become very inexpensive. If an organization has recently upgraded its data network, it may consider IPT.

- **Expiring Service Contracts**: The possibility of shifting some telephony expenses to the data network may be convenient when leases expire, but also adds leverage to bargaining power when renegotiating.

- **Voice Network Upgrades**: If the current voice network is not meeting business requirements it is a good opportunity to incrementally add and test new IPT services that will eventually lead to larger deployments.

- **Remote Users**: IPT can provide telephone support to telecommuters with high speed connections.

- **Company Merger**: When companies merge, they often bring together different telephony networks and technologies. Combining the two companies provides a unique opportunity to converge the networks as well (56-57).

No matter what the particular IPT implementation, there are certain characteristics that project teams must search for when acquiring IPT technology and services. Aside from meeting the network requirements discovered during planning and assessment, equipment must also be interoperable, non-proprietary, and easy to maintain. Services standards must be proven and enforced with measurable service level agreements (SLAs). Finally, an outsourced portion of the IPT deployment must be supported by strong relationships among providers. Enforcing these standards will assure long term viability of the IPT-based network.

- **Equipment**: To avoid additional costs and network difficulties, all IPT equipment should be non-proprietary and interoperable. The use of proprietary equipment often prevents equipment from different vendors from communicating correctly and can lock an organization into a position where they must continue to rely on one vendor for service. This lack of flexibility puts the business at the mercy of the vendor, creating the potential for inflated costs or system failure should the vendor company collapse or fail to keep up with business needs. An organization should support vendors that produce interoperable, open architecture systems. This facilitates the development of equipment that easily communicates between different types of networks, protocols, and vendor equipment. Until common standards are achieved, businesses should prefer equipment

that provides the most interoperability (e.g., IPT equipment that supports both SIP and H.323).

- **Services**: A SLA is an agreement between the user and a vendor that defines what services will be provided, at what cost, how they will be measured, and how deficiencies will be addressed (Newton 739). An organization must work with service vendors to create measurable SLAs that are easy to enforce (because they include specific actions when guarantees aren't fulfilled) (Robert Frances Group).

- **Outsourcing**: All of the practices discussed in this chapter could potentially be outsourced to another company. Outsourcing is the practice of hiring another company to handle an internal business function, usually because the organization believes that someone else can do it better at less cost. A company might outsource the entire IPT deployment, or just portions of it like the data network assessment or network upgrades. They might decide to bring in a system integrator as previously discussed. Almost anything can be outsourced.

An agency that outsources any of the IPT implementation or IPT services must work to create a relationship with the provider that will lead to long term success of the IPT deployment. This can be done by avoiding the following six mistakes: (1) Not clearly defining the desired results and how they'll be measured, (2) Not talking to a provider's current and former clients, (3) Failing to consider the long-term relationship dynamics, (4) Signing a standardized, multiyear contract, (5) Not planning up front for how the relationships might end, and (6) Treating the provider as an outsider (Walker 138).

### 6. Create an Implementation Plan

As previously mentioned, an effective method of implementing IPT is to make incremental adjustments. An IPT implementation plan is designed with this in mind and identifies distinct breaks in the process where effectiveness can be measured. A proven way to start the process is to conduct a pilot deployment. This gives the IPT project team the opportunity to gain experience with the technology before diving in to a full deployment. The pilot program helps the project team to truly understand how the IPT-based network will function in the organization and enables them to create an implementation plan that addresses the highest priorities first.

- **Pilot Deployment (Test Bed)**: A pilot program is a small implementation of IPT intended to be a learning opportunity that prepares for a larger implementation; however, it also helps to define a business case for IPT and to select the best equipment and services for a full deployment. The best place to perform the pilot is in a situation where there may be a high return on investment (see section C.5 of this chapter), where the potential for disruption is minimal, and where user cooperation and feedback is high. To get the most out of the test bed, the project team should learn as much as they can about the behavior of the system by experimenting with different equipment, configurations, traffic volumes, protocols, QoS mechanisms, and security mechanisms. They should understand how equipment from different vendors interoperates. They should understand how to recognize, isolate, and repair network problems. The experimentation should be supported with training and with strong working relationships with

potential vendors. Finally, the project team should be comfortable with the maintenance and long term management of the system to ensure success when vendor support fades. The more thorough the pilot program, the more prepared the project team will be for a large scale deployment of IPT (Walker 109-113).

### 7. Deployment

Once a pilot program has been conducted and an implementation plan is developed, the project team will be prepared to move into full deployment. The project team should begin to make adjustments to the network incrementally and be prepared for adjustments. Changes in the plan will effectively be recognized by building feedback loops into the process and by monitoring measurements that demonstrate system effectiveness (Yedwab). An example of a test plan that might be used to check each phase of the implementations is provided in Table 6. A systematic and continuous assessment of the implementation creates a smooth transition to a valuable IPT-based network.

| IPT Deployment Test Plan |
|---|
| • **Operation and Function**: Does all the end-user equipment work properly and provide all promised features?<br>• **Ease of Use**: Is the system easy for all users to use? Is the system easy for the IT staff to maintain?<br>• **Network Application Performance**: Is there good call quality?<br>• **Transaction-oriented Application Performance**: Are critical applications on the network still operating normally after the change? This requires the project team to take measurements prior to the change.<br>• **Settings**: Do equipment and applications still perform as expected after changing IPT configurations?<br>• **Stress**: Does the network provide good call quality to the predicted level of call volume? Does it transfer calls to the PSTN when the limit is reached?<br>• **Extraneous Traffic**: Is the system doing anything you don't expect or understand? A network protocol analyzer may help to determine this.<br>• **Reporting Problems**: Does the IPT management system operate correctly? Create faults in the system and see if the management system responds accordingly (Walker 116-118). |

Table 6. Sample IPT Deployment Test Plan

### 8. Network Management & Maintenance

Once the IPT-based network has been deployed, it requires constant attention to maintain high levels of reliability, call quality, and system security. An effective IPT management system will meet the future needs of a growing network while addressing four areas of concern: Operations, Availability, Call Quality, and Accounting. Security is an important piece of each area and must be consistently addressed to assure the well-being of the network (Walker 180).

#### *a. Managing Operations*

This section addresses some of the issues required to effectively manage daily operations and changes in the IPT network. It helps to understand how to identify and address the important problems proactively to prevent significant system failures. Three areas of focus will be discussed: configuration management, event management, and fault management.

- **Configuration Management**: A configuration is “the hardware and software arrangements that define a computer or telecommunications system and thus determine what the system will do and how well it will do it“ (Newton 203). To manage the IPT system configuration, the IT staff must: understand the current configuration, test and monitor all changes to the system configuration, closely track all changes, and limit and control who is authorized to make changes.

An awareness of the current system configuration is achieved through the use of readable and understandable files, reports, and diagrams. The network management team must understand what physical components make up the

network, they should know equipment specifics, and recognize how the components are linked together. This can be accomplished through the use of network topology diagrams and up-to-date inventories. Topology diagrams provide a good high-level understanding of how the network is connected. Inventories provide more specific information (e.g., name, location, addresses, function of the device, vendor, model, serial number, operating system version, available memory, processing speed, etc.) to better understand each components function in the network. There are also software tools available to help identify and track this information. Configuration files should be protected to ensure the current configuration is accurate. This is accomplished by limited access to authorized individuals, by backing up configuration files frequently, installing security mechanisms, and by closely monitoring access to the files in order to recognize potential damage (Walker 186-192).

- **Event Management**: Operating systems have the ability to track and log a variety of system events (e.g., opening, reading, modifying, and closing documents; when an application starts and stops; system errors). When system performance suffers, failures occur, or when the network has been attacked it is usually possible to recognize signs of the cause through system logs. There are so many logs to monitor that it would be infeasible to track them all, so an organization must prioritize what type of events are the most important to monitor. Then they must determine what kind of system response is required to address suspicious activity, which might include alerting the IT staff or executing corrective action without immediate human

intervention. It is wise to manage all of this information with software applications that help to track system events, consolidate logs, and help to recognize irregular activity (Walker 194-197).

- **Fault Management**: The IPT system management team must be able to locate and correct system problems quickly as a part of day-to-day operations to prevent significant downtime. The complexity of the network often makes it difficult to isolate problems. A team can do several things to locate problems more quickly. They should look in places where the most recent changes were made, in places where previous failures occurred, and in places where monitoring indicates a trend of increasing trouble. They may also identify the problem by tracking the logical path between two endpoints where the problem occurs. All problems, whether solved or still unidentified, should be tracked with an explanation of symptoms, expected time and cost to repair, solutions, and a priority. This will help the management team to address the most important problems first and create a repository of information that will enable faster resolution in later cases. Finally, the management team should have a plan to handle significant events, like a network failure or severe attack on security (e.g., DDoS), so that the problem can be addressed efficiently (i.e., decreasing the likelihood of long hours that can cause more failures due to human fatigue and limitations) before significantly impacting the business (Walker 197-200).

#### ***b. Maintaining High Availability***

An organization that desires a high level of availability must be committed to reducing network

downtime. This can be accomplished through prevention, detection, and reaction. The best approach is to prevent failures by actively responding to small indications of problems before they get out of control. When prevention is not successful, the IT team must be able to quickly isolate the problem so that it can be repaired. Once detected, the team must act quickly to provide a short term solution and follow up with a permanent fix and prevention of similar failures.

Though not all inclusive, there are two areas where an IT staff should focus for IPT-based networks. First, they must closely monitor IPT servers. Although servers can vary significantly depending on the functions they perform, they provide the most critical portions of the network. To enable good availability, these servers must be hardened as previously described and monitored continuously with a focus on the hardware, applications, and traffic. The second area of focus should be on managing applications. System software is complex and often acts unexpectedly, especially when interacting with other applications. Applications can often consume resources quickly or waste processing capability on unnecessary operations. Setting limits and closely monitoring these systems assists in achieving better levels of availability (Walker 200-204).

#### ***c. Maintaining Consistent Call Quality***

On initial deployment, the IPT-based network should provide satisfactory call quality. However, as the network grows and changes, call quality is likely to become an issue. To manage call quality, the IPT management team must first be able to measure and track current call

quality. Recall that toll quality is measured at an MOS of 4.0 or greater, while quality becomes unacceptable at levels lower than 3.6. Software is available to continuously monitor network traffic and determine an estimate of the MOS. Monitoring should occur throughout the network and trigger some kind of response, whether it be to alert staff or divert calls, when quality falls below established standards.

To prevent reductions in voice quality, IT staff should monitor network performance, enforce SLAs, tune QoS mechanisms, and plan for future growth. The network metrics for IPT that should be examined most closely are delay, jitter, and lost packets. Responding to fluctuations in these measurements help to maintain call quality. These measurements are typically used to establish service level agreements with service providers. Track them and hold vendors accountable to encourage consistent quality. QoS mechanisms must be managed to ensure that they are configured correctly and work correctly. The mechanisms can be complex, but can be managed with policy-based network management. A policy server monitors how traffic is handled and automatically generates and distributes configuration instructions that help components to apply QoS settings in accordance with policy. Finally, the network management team should prepare for future growth by tracking how the network responds when new users are added. Understanding these trends assists in determining how to incrementally install or upgrade components in response to increasing call demands. By focusing on network performance and future growth, an organization can consistently maintain call quality on the IPT-based network (Walker 205-212).

#### *d. Accounting*

Call detail records (CDRs) are used to keep track of the details of completed calls, containing information like the call source, destination, time, duration, delay, and jitter. The data can be used to monitor and troubleshoot the network, but are frequently utilized to determine who pays for the IPT service. This information must be tracked and monitored to ensure accurate billing and to help identify potential problems in the network. The information that is kept should also be protected, since it usually contains personal private information that is required by law. Prudent management of accounting records saves organizations money and assures compliance with privacy law.

Failure to successful monitor and upkeep the network can create substantial losses due to the costs of replacing damaged equipment, time lost by the IT staff, lowered employee productivity, and the loss of sales or customer trust. This is demonstrated by a Find/SVP survey in 2000 that estimated that Fortune 100 companies lost an average of $3 million (US) from network outages, not including the costs of lost productivity or missed calls (Walker 184). Good network management will come at an increased cost of human and physical resources, but is necessary to balance the risks of network failures that hamper business processes.

### 9. Manage Change

The final capabilities that are used in successful deployments are: the ability to manage the expectations of the people who will use the new system and the ability to adjust business practices to utilize new technology.

Company employees can be a great hindrance to any significant change in an organization, whether it is because they are comfortable with the old way of doing business or believe they will lose power or any other reason. The introduction of IPT will not only change the equipment in the business, but is likely to have an effect on how business is done in order to take full advantage of the opportunity. Agencies must harness the drive of those who are excited to implement the change and manage those employees who are likely to resist. Organizations that can do this throughout the implementation process are more likely to realize greater benefits from the IPT-based network.

There are many methodologies that have been created to manage this type of change in the organization, and most any of them could be applied to an IPT implementation. A framework for business transformation, which may be applied to IPT implementations, is explained by Joseph Kotter in the article, “Leading Change: Why Transformation Efforts Fail.” It consists of eight steps that are discussed below.

1) **Establishing a Sense of Urgency**: The urgency that must be conveyed for an IPT implementation is the opportunity to realize great benefits from a converged network. That urgency may soon be created by the need to stay competitive with other organizations that have already taken advantages of IPT-based networks. The level of urgency is established by the effectiveness of the business case made to stakeholders of an IPT system.

2) **Forming a Powerful Guiding Coalition**: The IPT implementation project team will lead the development, but can only do it effectively with the support (in the form of

money and power) of upper management. They can also drive positive change with the support of enthusiastic employees that have an interest in the end product.

3) **Creating a Vision**: The vision is supported by a strong business case and a well-planned implementation plan, which includes plans for development beyond the initial deployment and changes in business processes.

4) **Communicating a Vision**: All stakeholders, down to individual users, must have an understanding of the changes that will take place to convert to IPT technology and resultant business practices. This is accomplished through training and continuous communication that includes feedback between both implementers and users.

5) **Empowering Others to Act on the Vision**: This can be accomplished by getting full support from individuals who have the authority and budget to make changes. Enthusiast stakeholders will lose faith if not given the power to implement the IPT system the right way.

6) **Planning for and Creating Short-Term Wins**: Small deployments and pilot projects, which take advantage of great returns from small changes, will help to achieve buy-in from stakeholders. It is also an early indication of problems or resistance if a project team is unable to get user acceptance or realize business improvements on small changes. Successes, however, should be recognized to encourage further growth, acceptance, and positive business change.

7) **Consolidating Improvements and Producing Still More Change**: The incremental approach to implementing IPT-based networks described above provides an excellent method

to encourage change. The process produces gradual change in stages and confirms success through effective measures of performance. Not only must the technical aspects of the change be measured as described, but the project team must also monitor the effect those changes have on business processes. Incremental successes build upon each other to create more positive change and acceptance in the future.

8) **Institutionalizing New Approaches**: Finally, the implementation will be a success when stakeholders adjust to and accept new business processes created by the change in technology. Organizations should be wary of those who continue to reminisce about the way things used to be, and reward those who embrace the opportunity to improve business processes through the use of IPT.

THIS PAGE INTENTIONALLY LEFT BLANK

# V. COAST GUARD HEADQUARTERS CASE STUDY

## A. PURPOSE

Coast Guard Headquarters (CGHQ) Support Command (HSC) in Washington, D.C. administers telephony services for CG offices located at CGHQ and some others in the D.C. area. This chapter provides a background of HSC’s migration towards IPT in order to present an analysis of their security and implementation practices in Chapter VI. It includes a discussion of: the driving factors that led to the decision to begin implementation, the preparation conducted prior to deployment, the pilot project, the process of incrementally implementing IPT, and plans for the future. An understanding of the current implementation process at HSC facilitates the analysis of practices and assists in preparing for future deployments in the CG.

## B. BACKGROUND

### 1. Headquarters Support Command

HSC provides support services to HQ personnel and families via four divisions and other staff. This includes the Administration Services Division, which handles military personnel issues, facilities support and maintenance, procurement, property management and accounting, and work Life. The Command and Safety Division provides for the physical safety of personnel and equipment. The Clinical Services Division responds to personnel health care needs. Other staffs handle important support services like equal opportunity programs and religious services. Finally, the Information Services (IS) Division supports information technology needs by focusing on systems, customer support, budget and planning, and

communications operations. The IS Division is responsible for meeting the telephony needs of HSC and CGHQ, and currently does so through the use of the PSTN and other networks. They support various telecommunications functions by providing a Help Desk to respond to information service problems identified by HQ personnel.

**2. HQ Telephony Requirements**

The missions of each division briefly mentioned above and the various responsibilities of CGHQ offices combine to necessitate diverse telephony solutions that ensure operational effectiveness. Some of the services, equipment and features that are currently provided include: single line phones, multiple line phones, speaker phones, headsets, call hold, call transferring, call forwarding, intercom, redial, conferencing, Video Teleconferencing, remote access, secured telephone equipment and lines, 800 service, data lines (e.g., fax and modem), Octel VMX Voice Mail, broadcast messages, single digit menus (a.k.a. phone trees), pagers, cell phones, calling cards, GETS, simple dialing plans, and help desk services. In all, HSC services the needs of approximately 3600 telephone users (and 4000 numbers) to achieve mission performance at CGHQ.

**3. Department of Transportation (DoT) Telephony Services**

The majority of HQ's current telephony needs are provided by the PSTN via a local switch (PBX) owned and administered by the DoT. Among other government organizations in the D.C. area, the Coast Guard leases telephone lines and services from the DoT. This arrangement is similar to Centrex services previously discussed, where the DoT houses the equipment and provides services to other entities for a cost. Although this relieves the CG of the

burden of storing and maintaining the equipment, it has the disadvantage of reducing administrative control that delays configuration changes (e.g., Moves, Adds, and Changes (MACs)) and may increase the costs of services in the long run.

### C. CONSIDERING IPT

HSC was influenced by several factors when first contemplating the use of IPT. The primary factor prompting a change in telephony services is the fact that the Department of Transportation will be relocating to a new building in fiscal year 2007 with the intention of shutting down the local telephony switch that CGHQ currently operates on. Other factors include: the CG's transition from the DoT to the Department of Homeland Security, policy that supports moving away from legacy systems (i.e., aging PSTN equipment), the expansion of CGHQ into another building (Referred to as the Jemal or Half Street building), the potential (now confirmed) move of CGHQ within the next ten years, and mediocre telephony services provided by the DoT.

After learning of the DoT's future move, HSC was presented with three basic options; first, to shift to similar telephony services provided by the Federal Aviation Administration (FAA), or to stand up its own services with either a traditional solution or an IPT solution. The FAA solution was too expensive and relied too much on legacy equipment to be a viable solution, while the other two options appeared to be better long term solutions. The traditional solution would provide familiar and proven telephony services; however, HSC decided to move forward with an IPT solution because of the telecommunication

industry’s shift towards packet-switched technology and because IPT offered the features that most-suited the organization’s needs and promised to produce the best value.

The implementation of IPT addresses several of the concerns prompted by the DoT. It provides a new telephony solution independent of the DoT or other federal agencies, it is a progression away from legacy telephony equipment used by the CG, it is expected to provide portability and scalability that meets the needs of HQ expansion and relocation, and it offers enhanced feature sets that are expected to improve operational processes. Along with the services that the traditional PSTN system provides, the new IPT solution is anticipated to provide:

- Unified Messaging System: This is a service that supports the integration of email and voice messaging, allowing users to access voice messages (converted to text) via email or email messages (converted to voice) via the telephone.

- Improved Help Desk Services: IPT Call Management features facilitate the entering and monitoring of help tickets and trouble calls.

- Skill-based routing: This is a form of customer relations management and is commonly referred to as a phone tree. For HSC, the particular goal is to consolidate or centralize a variety of services at the Help Desk’s number at extension “HELP” (4357). For instance, a user might dial “one” to report data network problems (e.g., account access), “two” for telephone problems (e.g., echo), “three”

for facilities management (e.g., broken water fountain), and so on.

- Call Tracking and Monitoring: Tracking features of an IPT solution provides many advantages. First, network managers can more closely monitor telephone traffic to better understand requirements and make adjustments accordingly. It improves the measurement of performance metrics to hold service providers to established service level agreements. Finally, it improves the visibility of call records, allowing better tracking of call usage and billing, via TelSoft Solution’s MegaCall Call Accounting system. This is an improvement upon the previous relationship with the DoT where billing for use and services were often vague. Not only does improved billing information and tracking increase the potential for savings, but also provides a mechanism to offer services to other government agencies to reduce overall costs.

- Moves, Adds, and Changes: MACs are very slow and expensive, sometimes requiring weeks to complete. This is often created by the need to make physical changes to the PSTN to move an office for instance. The problem is further aggravated by sloppy wiring, necessary administrator involvement, and slow physical request routing processes. In contrast, a majority of MACs on an IPT network can be completed at the telephone terminal by the user in a matter of minutes or remotely by an administrator. An Improved MAC process provides significant savings in time and costs.

- Convergence: There are great potential benefits by bringing the data and voice networks together, particularly in the new Half Street building where there is

little interaction with the PSTN. It consolidates network equipment, management, and maintenance, effectively streamlining two different groups (data and telephony) to one more efficient team. Basically, HSC will be able to run its data and voice communications with the same personnel as before, but with increased control over functions that were previously controlled by DoT.

Despite the promise of several improvements through the use of IPT, HSC is not completely replacing the PSTN and will continue to utilize some its features in the near term. The reliability and proven stability of the PSTN will be utilized while both HSC and the telecommunications industry progresses to more complete IPT solutions. Specifically, HSC is incrementally replacing traditional telephony services with IPT services at the HQ building and is using the PSTN as a redundant form of communications in the new Half Street building. This process provides a known and reliable fallback as CGHQ transitions, it assures emergency communications during disasters, and it provides for emergency location services like E911.

### D. INITIAL PLANNING

After deciding to deploy IPT to meet HQ requirements, HSC began the planning process by selecting a project implementation team and by identifying the most appropriate equipment and services. After selecting a preliminary solution, HSC continues to test and evaluate elements of the IPT system to produce the best outcome.

- **Project Team**: The IPT project team consists of many existing members of the Information Services Division at HSC, including data network personnel, budget and finance functions, and security experts, with active upper

management involvement and support. The key to completing the team however, was the decision to contract telecommunications specialists with years of telephony experience and familiarity with packet-switched networks, and to outsource the system integrator function. HSC hired Connected Work Place Solutions (CWPS), a company that specializes in implementing 3Com IPT solutions, to facilitate a smooth transition into a new technology for the Coast Guard. This group of personnel provides a rounded out team of professionals equipped with the knowledge and expertise to deploy a secure and reliable telephone network at CGHQ.

- **Research & Vendor Selection**: HSC conducted extensive research to determine the best product for CGHQ's needs. This included market surveys, vendor site visits, and analysis of vendor documentation of equipment and past projects. Companies like Cisco Systems, Avaya, Nortel, 3Com, Sylantro, Broadsoft, and Qovia were represented. HSC also paid close attention to other agencies that had already implemented IPT, particularly the U.S. Fish and Wildlife Service because the scale and requirements of their solution was very similar to CGHQ needs.

HSC chose a solution provided by 3Com and supported by CWPS and Qovia. 3Com was selected because their products were most appropriate to the scale of the Coast Guard's implementation; whereas, companies like Cisco provided (and required) a lot of very expensive equipment more appropriate for large enterprise solutions. 3Com's equipment also proved to be more user-friendly. For instance, 3Com IP Telephones have "hard buttons" that allow the selection of an option at any time, where other vendors

often support equipment with “soft buttons” that only appear on the terminal after making other selections. Equipment from other vendors (e.g., Cisco routers) is being used to build the IPT-based network, but the core IPT components and endpoints have been produced by 3Com and implemented by CWPS. Qovia’s NetScout, an IPT network management tool, has also been selected for evaluation on the new packet-switched network. As HSC incrementally implements its IPT solution, it continually reevaluates the equipment and services provided by these vendors, as well as new products, to assure the best options are employed.

- **Preparing a Pilot program & the initial rollout**: After selecting an initial solution, HSC made preparations for a Pilot program in order to become familiar with the IPT technology and to test the IPT products provided by the selected vendors. HSC recognized the opportunity to improve its Help Desk functions, and chose to conduct a trial run by migrating approximately 40 Help Desk support personnel and services to IPT. They would follow this up with an initial rollout of IPT by moving approximately 300 personnel to the new Half Street building with new telephony services. After a successful trial program and rollout, HSC had plans to gradually migrate the remaining 3250 personnel at about 400-600 personnel every three months.

## E. HELP DESK TEST BED

To test and familiarize itself with IPT, HSC installed 3Com’s NBX call server, supporting telephone equipment, and call management software at the call center (Help Desk). The technology supports smaller IPT implementations primarily based on a 3Com protocol that is similar to the

H.323 protocol. It is used over the HQ LAN using the existing Help Desk extension.

Prior to implementation, the Help Desk was attended by two receptionists who processed phone calls, emails, and walk-in requests. They would answer simple questions, but spent most of their time entering remedy tickets into the system. The tickets would be prioritized by analysts in the back room who then worked to resolve them. The main problems with this method of resolving issues included the inability to capture all the information and the inability to respond in a timely manner. Information was often lost in this process because the two receptionists would become overburdened and forget to enter remedy tickets, personnel would choose not to leave a message when the two phone lines where tied up by the attendants, or an event (e.g., server down) would generate many calls that would not be added as remedy tickets because they related to the same problem and were too numerous to track.

One of the anticipated benefits of upgrading the call center with an IPT-based network was to be able to better track calls to more effectively meet the needs of those who call the Help Desk. The IPT system proved to improve the efficiency of the Help Desk. First, the call management software tracks all calls, whether they are live calls, voice messages, or even impatient hang ups. This information facilitates faster entry of remedy tickets and helps to track actual call volume to the Help Desk.

The business process of receiving calls also improved. There are still two receptionists at the front desk who handle most of the calls and walk-in requests, but now analysts in the back room are able to monitor activity of

the two attendants up front. When both of them are busy, analysts in the back room pick up the line and accept requests. As a result, more HSC customers are talking to live personnel, improving relations between support personnel and system users. Despite an increase in number of remedy tickets due to improved tracking, the Help Desk is now able to respond to requests in a timelier manner because of its ability to closely monitor and track incoming calls.

The Pilot demonstrated the benefits of other improved processes, like MACs. It increased mobility by allowing Help Desk personnel to move between phones by entering a personal access code, effectively logging into the phone. The pilot program successfully provided the opportunity to experiment and test the IPT equipment. It was particularly helpful to have some of those analysts, who would respond to IPT problem calls later, become comfortable with the use of the phones up front. IPT users and implementers quickly adapted to the use of the new phone systems and made minor adjustments (e.g., echo was a common problem) to tune the network to optimum performance.

## F. INCREMENTAL DEPLOYMENT & TESTING

Upon completion of a successful pilot program, HSC continued to move forward by making plans to move the Coast Guard Acquisitions Directorate and the Coast Guard Deepwater Directorate to the new building where a new IPT-based network would be installed. The Acquisitions Directorate is responsible for the acquisition of large Coast Guard assets, like Aircraft, Cutters, small boats, and facilities. The Deepwater Directorate is responsible for conducting the Integrated Deepwater System Program:

> an integrated performance-based approach for upgrading existing assets while transitioning to newer, more capable platforms with improved systems,…recapitalizing the Coast Guard's aging deepwater assets and support systems by modernizing or replacing with state-of-the-market interoperable systems (IDS).

The two of these directorates combined contain over 300 telephony users with a wide variety of telephony needs. Before starting the shift to internet protocol telephony, HSC prepared both directorates with briefings of planned changes, user training, and through the production and distribution of brochures and user manuals.

The transition of these CG organizations would require the shift of all offices and equipment to the new building. This transition would benefit the IPT implementation on one hand, by creating one large change for personnel to deal with at one time (over the weekend), rather than making several encumbering adjustments over a period of time. However, it increased the possibility of unanticipated events that could be more difficult to handle due to the increased workload during the transfer. In fact, the change over required a new dial plan with new phone numbers for each user. Due to a few minor human errors, the phone list was completely incorrect and many individuals where moved to the wrong physical location, significantly impacting the original dialing plan. Fortunately, the capability and features of the new IPT solution demonstrated the ability to quickly makes changes and restore the system to order in one evening.

The relocation was also complicated by the unknowns of transferring to a new facility. Potential issues that were resolved or became insignificant were: a tight building

construction schedule, the collapse of fiber optic ducts, and renegotiation of telephony service contracts. Fortunately, construction completed on time, the fiber lines were led overhead and backed up with line of sight transmission via optical laser (eventually a third fiber connection was established through power ducts), and the shift to IPT encouraged competitive pricing among service providers in the area.

The two Coast Guard Directorates smoothly transitioned to the Half Street building without major incident and without loss of telephony services. At peak hours of use they approach approximately five percent bandwidth utilization, although that is likely to change near the end of the fiscal year for these Directorates. The current IPT solution provides most of the features, functionality and bandwidth required by the current users with room for growth for future implementation of IPT at CGHQ. HSC is currently evaluating the initial rollout of these Directorates and plans to shift the remainder of HQ personnel to the IPT solution, followed by an incremental increase in call features that weren’t available with the first deployment. Their future plans will be discussed after a description of the current IPT network is presented.

## G. IPT NETWORK DESCRIPTION

The network depicted is not an exact representation of CGHQ’s actual IPT network, but provides enough description to encourage an understanding of the basic operation of the network and still maintain an appropriate level of security.

Both the CGHQ building and the Half Street building have similar network characteristics throughout with a few variations of equipment. Similarities include the physical protection of the network, where both buildings incorporate security mechanisms that protect critical pieces of the network. Equipment resiliency is supported by backup systems like RAID (redundant array of independent disks) drives, universal power sources, generators, and system backups. Both buildings also provide logical protection of information by separating voice and data on separate virtual local area networks. The voice data itself never leaves the LAN via the internet; rather, the IP phone sets up external calls through the PSTN by way of the Call Processor and Gateway as illustrated in Figure 8 (Section II.3). Finally, the IPT-based network is supported by the PSTN, providing E911 services, analog capability (e.g., fax and modem), and an automatic transfer to the PSTN should the IPT network fail.

### 1. CGHQ Building

The primary IPT equipment located in the CGHQ building is listed below with a description of basic function and security functions.

- 3Com Linux Appliances: All of the 3Com IPT server equipment described below (including the Half Street building) are produced and maintained by 3Com. They are treated like appliances, where 3Com hardens machines and replaces equipment as necessary. This reduces the effort of constant system patches and upgrades, and is believed to be more secure than other systems (i.e., Microsoft based machines). These machines are devoted to the IPT applications described and have any other unnecessary

services disabled. They have the ability to produce messages and alerts during system failures. Each machine is also backed up with a universal power supply.

- 3Com NBX Call Control Server: This server is the gateway between the PSTN and the HQ LAN for the HSC Call Center (Help Desk), and is intended to serve small IPT implementations. It provides 1500 ports, has mirrored hard drive, is backed up by the VCX (see below) server during failure, and provides filtering (firewall) capability.

- 3Com VCX Call Control Server: This server is the gateway between the PSTN and the HQ LAN for all other users and provides for a larger scale implementation. It provides 10,000 ports, RAID for processing redundancy, is mirrored by another VCX server in the Half Street building in case of system failure, and provides filtering (firewall) capability.

- 3Com Unified Messaging System Server: The UMS server provides voice mail services for HQ users, with the capability of accessing and converting the format of both voice mail and email. This server is mirrored by another UMS server in the Half Street building and has RAID for processing redundancy.

- Telemanagement Server: This server provides the billing and accounting service for the IPT at HQ. It uses TelSoft software call MegaCall to perform these functions. For redundancy it has RAID drives and routine backups.

- Security Server: This server is the only machine described that is not entirely used for IPT services. It resides on the data network and manages security policies all data network and IPT machines. It alerts support

personnel and provides “advice” (e.g., pictures, maps, schematic, and priority of alarms) to personnel on duty who are unfamiliar with the alarms.

- IPT Telephones: Telephone terminals are all 3Com handsets that provides varying functionality based on the model. They do not provide fax, modem, or other analog capabilities. No wireless handsets or Softphones are currently being used or allowed on the network.

- PSTN: The PSTN provides for fax, modem, and other analog services. It also provides for E911 location services. It serves as fall back when IPT services fail.

**2. Jemal (Half Street) Building**

- The Half Street building also has a 3Com VCX Call Control Server and a 3Com UMS Server that mirror the servers at the HQ building. They provide primary service to IPT users, while being mirrored and effectively backed up by the servers at the HQ building.

- The IPT Telephones and PSTN features described for the HQ building are provided for at the Half Street building.

- The Half Street building does not have backup generator power for IPT equipment in the building. All equipment has backup power that provides time for safe system shut downs but will not allow extended processing capability.

**3. Network Links**

The two HQ buildings are physically linked through several points of access. These links are provided by fiber cable that is either run through power ducting, fiber cable that is run through telephony ducting and routed above

ground along telephone poles to bypass collapsed ducting, or passed through the atmosphere by line of sight optical lasers positioned on top of each building.

#### 4. Diagram

The following diagram (Figure 10) shows the basic logical (and some physical) setup of the IPT network. The call control servers provide a gateway between the IPT network and the PSTN, while also allowing analog services through the PSTN. The rest of the IPT equipment is basically on an Ethernet backbone, subnetted on one VLAN to segregate it from the data network. The data network resides on the CGDN, the Coast Guard's Intranet, which is connected to the Public Internet through connections that are managed and protected (via firewall and other security mechanisms) by the Coast Guard Telecommunications Command (TISCOM). Connection to the HQ IPT VLAN for remote configuration management of IPT equipment is performed via a Remote Access Server (RAS) that resides at TISCOM.

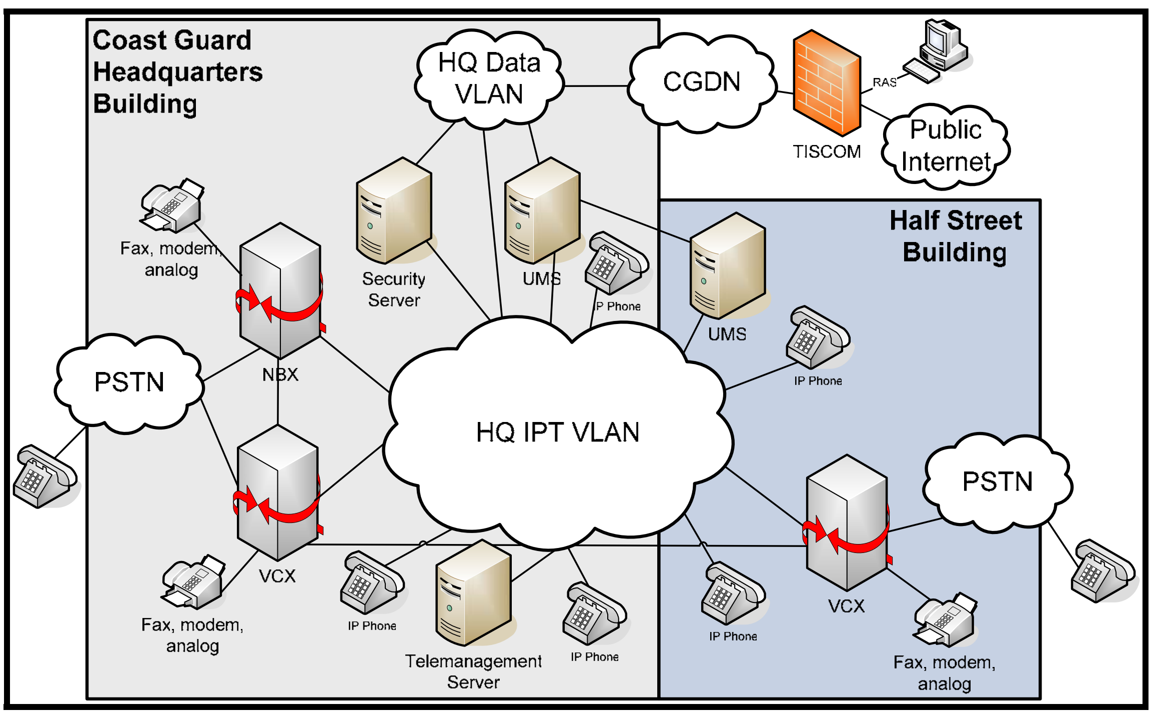


Figure 10. CG Headquarters IPT Network Diagram

## H. FUTURE DEVELOPMENT

HSC will work to transfer the rest of CGHQ to an IPT telephony solution beginning in July of 2005. They plan to shift approximately 400 to 600 people every three months until the remaining 3250 users are utilizing IPT services. The process will include continual monitoring of system resources and capabilities, via Qovia’s NetScout and through the stand-up of a Network Operations Center (NOC), to assure call quality and maintain security. There are also plans to create “fly away” kits that allow remote IPT service to support continuity of operations (COOP) planning when natural or man-made disasters occur. When complete, this IPT solution of the CGHQ local area network will be the first step towards larger Coast Guard enterprise implementation of internet protocol telephony.

Following full integration of CGHQ, HSC is likely to provide IPT service to the National Response Center (NRC). The NRC is the sole federal point of contact for reporting oil and chemical spills. Careful planning is required to meet the NRC’s requirement of 24 hour telephony service without interruption. Transition to IPT must be watertight, but will provide great benefit once established by supporting the NRC’s Incident Response Information System (IRIS). IPT integration with IRIS will allow quick dialing, quick production of reports, voice recording, call labeling, and generation of call statistics. These capabilities greatly improve NRC’s ability to respond to environmental catastrophes. HSC also plans to equip the Coast Guard Command Center and other commands with the same kind of operational capabilities provided by an IPT solution.

Once the Coast Guard has established IPT networks among units on HQ’s local area network, the next logical step would be the deployment of IPT across the Coast Guard’s Data Network (Intranet) followed by the eventual transport of voice data across the Internet. The long term goal is to provide the benefits of IPT to all aspects of the Coast Guard’s resources, from the smallest and most remote CG Station to the largest CG command, to assets afloat and ashore, both nationwide and worldwide. Through its initial development of IPT, HSC has positioned the Coast Guard well for a transition to the supposed future of telecommunications.

# VI. CASE ANALYSIS

## A. PURPOSE

The purpose of this chapter is to analyze HSC’s deployment of IPT with respect to the security policy and implementation practices discussed in this document. First, the use of security mechanisms will be evaluated based on: Physical Security, Logical Separation, Network Traffic Management, IPT Equipment, Encryption and Authentication, and Redundancy. For each attribute, strengths and weaknesses will be identified as appropriate and recommendations made to encourage better security. Implementations practices will be explored in the same manner, with a focus on: Forming an Implementation Team, Understanding Telephony Requirements, Understanding the Data Network Infrastructure, Updating the Data Network, Developing a Business Case and Acquiring, Creating an Implementation Plan, Deploying IPT, Network Management and Maintenance, and Managing Change.

## B. SECURITY

### 1. Physical Security

The physical security mechanisms employed at CGHQ provide the expected level of security for all elements of the IPT network. Some of the equipment and methods used to protect critical components of the network include: automated monitoring systems, closed circuit television, motion sensing cameras, system disconnect alarms, power loss alarms, flooding alarms, HVAC, chemical biological protection, door position switches, door strikes, motion sensors, proximity card readers, and security guards. To the greatest extent possible, cabling and data transport

media are protected by physical barriers to prevent unauthorized physical access to the network.

- **Recommendations**: The physical security measures set up at CGHQ will effectively deter most physical attacks on the voice network. To maintain strong protection, HSC must ensure those mechanisms are not weakened through human complacency (e.g., failure to log and escort visitors, bypassing authentication systems by holding the door open for other personnel, ignoring alarms, etc.). HSC should develop and enforce policy that supports the proper use of these physical protections and barriers.

**2. Logical Separation**

To err on the side of security and prevent potential attacks on the voice network from data network vulnerabilities, HSC initially installed physically separate data and voice transport media in the Half Street building. That is, different cabling is provided for data and voice. This reduced some of the cost savings of a converged network, but provided better security. HSC recognized that adequate security could be provided by logically segregating the network and use common physical components. As new development occurs in the new building, all data and voice equipment will support only one physical network, but divide voice and data traffic through the use of separate subnets (VLANs).

There are currently no softphones or wireless IP Phones on the IPT network. This reduces the number of potential threats on the network through interaction of different networks (i.e., voice, data, wireless). The UMS server, security server, and network switches are the only

places where the voice and data networks interface. These points are not supported with Intrusion Detection Systems.

- **Recommendations**: Separation between the data and voice networks has been established on the CGHQ network, providing adequate security to the IPT-based network. To maintain security and call quality, HSC must actively monitor the network to ensure that unused ports are closed (especially data network ports on IPT equipment), that data and voice packets remain on separate VLANs, and that unauthorized equipment that compromises network segregation(e.g., personal softphone agent software) is not added to the network.

**3. Network Traffic Management**

The IPT VLAN resides within the HQ data network LAN, which is a part of the CGDN. The CGDN accesses the public Internet through firewalls that are controlled by TISCOM. It is assumed that the CGDN is relatively secure from external influence and that all traffic residing on the CGDN is trusted; therefore, there are few filtering or IDS mechanisms within Headquarter's IPT solution.

Since the IPT network connects directly to the PSTN via the VCX and NBX gateways, there is no need to use Network Address Translation between the HQ IPT LAN and any other networks. This reduces the complexity of securing IPT conversations that traverse different networks.

IPT Equipment and Servers may be configured remotely by a small number of administrative personnel. They gain access to the IPT network by connecting to a Remote Access Server (RAS) from their home (or remote) computer. This provides a secure connection to the CGDN.

- **Recommendations**: The CGHQ IPT solution will require more preparation before it can complete calls over the Internet or other untrusted networks. Since it is assumed that all information on the CGDN is trusted, HSC has put few mechanisms in place to separate the voice network from other influences. The use of separate VLANs is adequate for the current implementation over the HQ LAN; however, HSC must use firewalls, IDSs, and other network monitoring equipment to assure good call quality and security for calls that will traverse other networks. The Coast Guard should balance the costs of implementing these security mechanisms prior to moving voice over the public Internet.

#### 4. IPT Equipment

As described in the previous chapter, the IPT servers have been hardened by the manufacturer and are replaced as an entire “appliance” when upgrades are necessary. They are generally designed and used for one application. HSC can strengthen the security of these machines by utilizing built in firewall, intrusion detection, and alerting systems and by disabling unnecessary services.

Other IPT equipment, like switches, routers, and IP phones, have been hardened by disabling unused ports and services, and by maintaining up to date patches and antivirus software. They require access through authentication mechanisms to make configuration changes.

- **Recommendations**: CGHQ has a good start by using strong equipment. They must continue to monitor the equipment and ensure built-in security mechanisms are utilized to maximize security, reliability, and call quality.

### 4. Encryption and Authentication

Voice encryption is not currently being utilized on the IPT network because voice conversations do not leave the LAN on a packet-switched network. It is assumed that the risk of overhearing an unclassified conversation and the subsequent consequences are acceptable (a greater risk is the employee that is too loud).

Authentication mechanisms are in place on all IPT Phones and equipment to assure trusted personnel access the equipment. For instance, each user has an account and a personal code that they must use to logon to a IP Telephone.

IPT Equipment and Servers may be configured remotely by a small number of administrative personnel. They gain access to the IPT network by connecting to a Remote Access Server (RAS) from their home (or remote) computer. This provides a secure connection to the CGDN.

- **Recommendations**: As the Coast Guard expands it IPT capability, it must prepare to provide more encryption and authentication mechanisms. The current solution would not adequately protect call conversations over the Internet and achieve the desired call quality.

### 5. Redundancy

The IPT-based network at CGHQ ensures reliability by employing several points of redundancy. With the exception of consistent generator power in the Half Street building, all critical equipment is backed up with emergency power to allow continuous operation during losses of power. At a minimum, all vital components are backed up with power sources that allow sufficient time for safe shut downs. Power failure tests are conducted regularly. To assure

system processes stay online, critical IPT equipment files are backed up or stored in redundant memory locations. Vital servers are mirrored or backed up by other servers to ensure operations during system failure. When the IPT network fails, the voice network automatically faults over to the PSTN to provide telephony services. Finally, disaster recovery planning is conducted regularly in order to provide continuity of operations.

- **Recommendations**: Generator power at the Half Street building has not been established. To ensure better reliability of the voice network, HSC should work to quickly bring long term backup power to the building. Otherwise, the current support mechanisms provide the means to maintain a reliable network.

## C. IMPLEMENTATION PRACTICES

### 1. Forming an Implementation Team

HSC developed a strong project team consisting of individuals with a variety of background and experience. The areas of specialty brought by members of the team included: past Coast Guard or CG headquarters experience, telecommunications, internet protocol telephony, traditional telephony, data network management, data network security, computer security, physical security, budget and finance, facilities engineering, and others. The decision to outsource the role of system integration to a company experienced with 3Com equipment and IPT greatly strengthened the ability of the implementation crew. A focus on the selection of experienced project team leaders led to a very smooth and effective implementation of IPT.

- **Recommendations**: To maintain a high level of IPT security and call quality, HSC must continue to educate and

train its network management personnel and maintain strong relationships with its telecommunications carriers, contracted support personnel, and system integrators. The experience and diligence of these personnel will keep the system running in the long term.

**2. Understanding Telephony Requirements**

Some members of the project team already had years of experience with traditional telephone use at CGHQ and were immediately able to transfer that knowledge towards the preparation of requirements for an IPT-based network solution. They immediately recognized the potential benefits that IPT could provide to MACs, telephony feature sets, and telecommunications contracts with service providers.

- **Recommendations**: Telephony requirements are likely to change as organizations within the Coast Guard realize the benefits of new features that IPT provides. As the technology advances and as personnel become more familiar with it, business processes and use of telephony are likely to change. Network managers should continually monitor network traffic and work with stake holders to understand requirements and adjust accordingly.

**3. Understanding the Data Network Infrastructure and Updating the Data Network**

The benefit of deploying IPT at a new facility is that it saves the effort of analyzing and upgrading the old data network. Installation of the test bed and other IPT services at the old HQ building, however, required an examination of the network. HSC’s study and preparation of the network and its available bandwidth allowed a smooth transition to a new centralized Help Desk. Increased bandwidth and the use of QoS mechanisms helped to improve

the flow of voice over the data network. Telephone services, features, and call quality introduced by the new IPT system proved to meet the needs of its users.

- **Recommendations**: As CGHQ transitions more users from the PSTN to the new IPT-based network, it must continually monitor the data network and its interaction with the voice network to assure the security of the IPT network. They should be prepared to make adjustments to the data network to handle negative interactions or increased traffic volume caused by the introduction of IPT. They must be especially diligent when they move to the point where they are moving voice conversations over the Internet.

#### 4. Developing a Business Case and Acquiring

HSC had several good reasons to switch to IPT. First, a need, which might be considered an opportunity in this case, presented itself when the DoT announced that it would be moving and shutting down its switch. Second, the DoT’s move coincided with CG pressure to move away from old processes (e.g., relationships with DoT) and legacy systems. Third, the expansion of CGHQ to another building and a future CGHQ move encouraged the consideration of a new and portable technology. Finally, the combination of these demands and opportunities brought the realization that new technology could bring cost savings and improved productivity through features like unified messaging, inexpensive MACs, and convergence.

The project team conducted thorough reviews of many IPT vendors and the equipment and services provided. They also researched other implementations to understand the kind of capabilities, limitations, features, and requirements inherent in an IPT solution developed for

organizations with similar missions and size. Careful consideration of these factors helped HSC to choose a product by 3Com that appeared to fit well, was interoperable (via SIP standard), and provided scalability to prepare for IPT growth in the Coast Guard. The implementation of this product was supported by the selection of a system integrator that was charged with ensuring a smooth installation and sustainined maintainability by providing training and documentation. An IPT-based network management tool, Qovia’s NetScout, was also acquired to monitor and manage the IPT network for long term viability. Finally, service contracts with telecommunications service providers were negotiated to guarantee the bandwidth required to support the IPT network in the near future.

- **Recommendations**: Although the use of IPT is growing, some organizations are still slow to change due to the reliability and quality already provided by the PSTN. CGHQ must demonstrate successes to encourage the spread of IPT throughout the Coast Guard. As IPT grows in the CG, telecommunications managers must choose equipment and services that are interoperable and scalable. The systems must be able to grow with the technology and interact with other IPT systems to assure communications between CG units and other government agencies.

### 5. Creating an Implementation Plan

The pilot program conducted at HSC’s Help Desk was invaluable in preparing the IPT implementation team for the rollout of IPT at CGHQ. Many of the personnel working at the Help Desk were the same people who would be installing and supporting the IPT solution for CGHQ. The test bed

allowed these employees to understand how to address voice network problems and tune the IPT system to bring maximum performance. They were also better able to understand user questions and concerns, through their own experiences with the equipment. Additionally, the pilot program measured and confirmed the capability of the data network, vendor equipment, and workforce aptitude.

- **Recommendations**: CGHQ should continue to experiment and learn as it continues to transition to a full IPT solution. The same careful planning and experimentation must take place before the CG begins implementation across the CGDN and again before utilizing IPT across the Internet.

**6. Deploying IPT**

The key success of HSC's deployment to date is its incremental approach to implementation. Each stage of the process has been carefully laid out, performed, and then tested. A gradual approach to full deployment allows the project team to properly plan, to respond to and resolve unanticipated events, and to confirm satisfactory operation. Attempting to implement the entire system at once can: overwhelm the implementation team, make it more difficult to isolate problems, frustrate users, increase security risks, hamper the data network, and increase the risk of failure. A controlled approach allows the project team to adapt to changing requirements and the rapidly changing IPT technology with reduced risks.

It is important to reiterate that incremental adjustments to the IPT system must be followed by rigorous testing. If implementers fail to test changes, then the strength of the incremental approach quickly weakens.

Assuming that changes or updates will flow smoothly can lead to failure. For instance, the potential threat of this type of problem was illustrated during implementation on HQ backup generators. It was believed and assumed that many pieces of critical IPT equipment were connected to and backed up with generator power. A power failure test revealed that they were not, in fact, backed-up adequately and they shut down. Fortunately, it demonstrated the ability of the mirrored server setup when the backup servers came online, but put undue stress on the IPT equipment. Continuous monitoring and testing practices must be maintained to prevent these types of problems.

- **Recommendations**: The method of deployment must be monitored and balanced to achieve greater value and to reduce risk. As the IPT project team becomes more proficient, it may be appropriate to expand services more quickly. On the other hand, if telephony requirements or IPT technology change significantly, then the team may consider smaller increments.

### 7. Network Management and Maintenance

HSC uses software (e.g., Qovia tools and NetScout)to monitor network traffic, bandwidth, and equipment. These tools help to make adjustments to the network to assure call quality and reliability. HSC continues to research better traffic management products in order to maintain the network more efficiently.

The Coast Guard currently uses the Remedy ticket system to handle problems and conduct configuration management on the voice network. They are in the process of researching a more robust application (that utilizes

advanced detection, monitoring, and alarm capabilities) to manage network failures and updates.

- **Recommendations**: HSC will be more capable of maintaining a strong IPT-based network in the long run when it implements stronger traffic management and configuration management systems.

**8. Managing Change**

The decision to shift towards IPT was driven by a great opportunity to improve telephony features when the legacy telephone systems were going to be replaced. HSC capitalized on the opportunity by putting together a strong team to lead the development. The team had the authority, funding, motivation, and experience to drive successful change in the organization. Bringing new personnel from outside of the organization brought fresh ideas and enthusiasm. Training and user involvement encouraged buy-in from all levels. And the successes of the pilot program and the initial rollout have bolstered efforts and will help to push IPT through full deployment at CGHQ.

- **Recommendations**: The acceptance of IPT and its improved capabilities appear to have taken hold at CGHQ. To gain further success throughout the Coast Guard, those who wish to push voice and data convergence forward must consider how to manage the adjustment. The reliability, security, familiarity and call quality of the PSTN often hinder consideration of IPT technology. Addressing those issues and demonstrating consistent successes and improvements in IPT will help to encourage convergence.

# VII. CONCLUSIONS AND RECOMMENDATIONS

## A. REVIEW

This thesis has explained the basic operation and components of the PSTN and an IPT-based network in order to facilitate the discussion of IPT security and deployment. Potential threats and vulnerabilities specific to IPT were enumerated, as well as the consequences of successful attacks on IPT phone calls. Then safeguards and other security mechanisms were listed to prevent attacks on the network, with an understanding that implementation of those security tools often comes at a trade-off, whether it be cost, voice quality, or some other desired trait. After addressing security, desired characteristics of an IPT-network were explained, followed by the practices that organizations use to successfully produce those qualities.

With that background, a specific IPT implementation by Coast Guard Headquarters Support Command at Coast Guard Headquarters was studied with respect to security and deployment practices. A description of CGHQ’s background and telephony requirements were given, as well as portrayal of the process that HSC used to implement a test bed and initial rollout of the IPT technology. Finally, HSC’s implementation processes and use of security measures were analyzed to help understand how the rest of the Coast Guard could learn from those experiences.

## B. LESSONS LEARNED

HSC took a cautious approach to implement an evolving information technology. The use of IPT promised to introduce increased capability through decreased costs and improved operations. However, a simple switch could not be

made without consideration of issues like security, reliability and call quality. These concerns were characteristics that were often taken for granted in the PSTN. Through careful planning and an incremental implementation process, HSC demonstrated that IPT-based networks can effectively replace many portions of the PSTN (However, in this case, IPT does depend on the PSTN for external calls, E911, fax, modem, and backup capability). That is, on the CGHQ LAN, the IPT-based network can provide acceptable levels of reliability, security, and call quality while providing extra features not available on the PSTN.

Despite the success of the first stages of the implementation at CGHQ, the results cannot necessarily be extrapolated to all situations. This particular deployment occurred on a relatively small scale on a simple set of systems. It only extended across CGHQ’s LAN. It did not extend across the CG’s WAN (CGDN) nor move across the Internet. It did not provide E911 location service, secure communications, or service to analog equipment (e.g., fax, modem). The mention of a few of the potential differences between IPT systems demonstrates how widely different agency’s requirements and solutions may vary. Therefore, each IPT implementation must be carefully planned to meet the needs of an organization and to adjust to the changes in IPT technology. No two solutions are similar; however, a common set of approaches may be used to bring about successful IPT-based systems.

The IPT deployment at CGHQ was successful to date because of a meticulous planning phase and an incremental process of expansion and improvement. HSC’s initial

deployment was simple precisely because it was designed to be that way. The project team understood the various risks associated with various deployment options and chose a conservative path based on the CG’s inexperience with this changing technology. CGHQ has a good start on introducing IPT technology to the Coast Guard through this initial implementation and must continue to vigilantly plan, make incremental improvements, and test. This approach will ensure that the Coast Guard implements the IPT solution that provides the most organizational value, but still provides good call quality, security, and reliability.

## C. FUTURE WORK

Since HSC focused on a relatively limited IPT solution to introduce the Coast Guard to IPT, there are many other areas where the technology may be investigated to encourage further progress:

- Are acceptable levels of call quality, reliability, and security viable across other networks, including: the CGDN, the Internet, and classified networks?

- Are acceptable levels of call quality, reliability and security viable across different media, including: wireless connections, satellite communications, and shipboard radio communications?

- Are converged networks actually the wave of the future, as most believe, or just a passing fad? Are government agencies jumping on the bandwagon too soon or are they falling behind?

- What protocols will emerge as the dominant standards among IPT equipment and services? What type of equipment and services must government agencies acquire to

develop IPT architectures that support interoperability and information sharing.

# LIST OF REFERENCES

Arkin, Ofir. “Security threats to IP telephony-based networks.” ;login: Magazine. 27 (2002): 30-36.

Arkin, Ofir. “Why E.T. Can’t Phone Home? Security Risk Factors with IP telephony based Networks.” Sys-Security Group Whitepaper. November 2002. <www.sys-security.com/archive/papers/Security_Risk_Factors_with_IP_Telephony_based_Networks.pdf>.

Carlberg, Ken. “Framework for Supporting ETS in IP Telephony: Internet Draft.” Internet Engineering Taskforce. 5 February 2004. Accessed 1 July 2004 <www.ietf.org/ietf/1id-abstracts.txt>.

Cisco. “Security in SIP-Based Networks.” Cisco Systems Whitepaper. Accessed 14 June 2004 <www.cisco.com/en/US/tech/tk652/tk701/technologies_white_paper09186a00800ae41c.shtml>.

Davidson, Jonathan and James Peters. Voice Over IP Fundamentals: A Systematic Approach to Understanding the Basics of Voice over IP. Indianapolis: Cisco Press, 2000.

Defense Information Systems Agency (DISA). “Voice Over Internet Protocol (VOIP) Security Technical Implementation Guide.” Version 1, Release 1. 13 January 2004.

Department of Homeland Security. “Interim Management Directive System IMD Number: 4600: Personal Use of Government Office Equipment.”

Estes, Tom. Personal Interviews. 15-17 December 2004. 17-18 March 2005.

Integrated Deepwater System (IDS). Accessed 15 March 2005. <http://www.uscg.mil/hq/g-a/Deepwater/program/intro.htm>.

Integrated Research. “IP Telephony Market Study: September 2004.” www.ir.com. Integrated Research: September 2004.

Joch, Alan. “IP telephony a step at a time: New hybrid phone gear calms transition fears.” 28 July 2003. FCW.com. Accessed 29 September 2004 <www.fcw.com/fcw/articles/2003/0728/tec-tele-07-28-03.asp>.

Keneipp, Ray. “Is IP Telephony Secure Enough for Enterprise Deployment?” Burton Group Research Overview. <www.burtongroup.com> 20 March 2003.

Kotter, John P. “Leading Change: Why Transformation Efforts Fail.” Harvard Business Review. March-April (1995): 59-67.

Kuhn, D. Richard, Thomas J. Walsh and Steffen Fries. “Special Publication 800-58: Security Considerations for Voice Over IP Systems: Recommendations of the National Institute of Standards and Technology.” National Institute of Standards and Technology, Technology Administration, U.S. Department of Commerce. April 2004.

Mairs, John. VPNs: A Beginner’s Guide. Osborne: McGraw-Hill, 2002.

McKnight, Lee W., William Lehr and David D. Clark, Eds. Internet Telephony. Cambridge: MIT Press, 2001.

Miller, Mark A. Voice over IP Technologies: Building the Converged Network. New York: M&T Books, 2002.

Murray, William Hugh. CS3670: Secure Management of Systems Course and Instructor Notes. Spring 2004.

Newton, Harry. Newton’s Telecom Dictionary. 20th ed. San Francisco: CMP Books, 2004.

Passmore, David. “SIP for VoIP: Not Just Another Protocol.” Burton Group Network and Telecom Strategy Report. <www.burtongroup.com> 21 February 2002.

Poulsen, Kevin. “VoIP Hackers Gut Caller ID.” The Register. 7 July 2004. Accessed 22 October 2004 <www.theregister.co.uk/2004/07/07/hackers_gut_voip/print.html>.

Power, Richard. Tangled Web: Tales of Digital Crime from the Shadows of Cyberspace. Indianapolis: Que Corporation, 2000.

Ragsdale, Gary L., Gerard P. Lynch, and Michael W. Raschke. "National Communications System Techinical Information Bulletin 00-8: The Convergence of Signaling System 7 and Voice-over-IP." National Communciations System. September 2000.

Robert Frances Group. “Enterprise VoIP Update – Taking It One Step at a Time.” RFG. 1 October 2002. Accessed 1 August 2004 <www.rfgonline.com/subsforum/archive/daily/093002/100102nt.html>.

United States Coast Guard. “COMDTINST 5230.56: Policy on Coast Guard use of Internet/Worldwide Web.”

United States Coast Guard. “COMDTINST 5375.1A: Limited Personal Use of Government Office Equipment.” 6 April 2004.

United States Coast Guard. “COMDTINST M5500.13B: Information Assurance Manual.” 29 March 2004.

United States Coast Guard. “COMDTINST M5530.1C: Physical Security and Force Protection Program.” 17 December 2001.

Varshney, Upkar, Andy Snow, Matt McGivern and Christi Howard. “Voice Over IP.” Communications of the ACM. 45 (2002): 89-96.

Walker, John Q. and Jeffrey T. Hicks. Taking Charge of Your VoIP Project. Indianapolis: Cisco Press, 2004.

Yedweb, David H. “An 11-step program for enterprise VoIP implementation: Part 2.” TelephonyOnline.com. 11 June 2004. Accessed 1 August 2004 <telephonyonline.com/ar/telecom_step_program_successful/index.htm>.

THIS PAGE INTENTIONALLY LEFT BLANK

# BIBLIOGRAPHY

Abbasi, Arsalan H. "Voice over IP: A Discussion of Business and IT Challenges." Wesley J. Howe School of Technology Management. Stevens Institute of Technology. 16 December 2003.

Alcatel. “IP Telephony Design Guide.” Alcatel Whitepaper. April 2003.

Alleyne, Audrey. Personal Interview. 15 December 2004.

Anonymous. “Case Studies on Early Adopters of Emerging Technologies.” Working Council for Chief Information Officers. <www.cio.executiveboard.com> January 2004.

Anonymous. “Information Note IN03-001: Securing VoIP.” Government of Canada, Office of Critical Infrastructure Protection and Emergency Preparedness. 13 June 2003.

Anonymous. “IP Telephony.” Burton Group Reference Architecture Technical Position. <www.burtongroup.com> 25 August 2004.

Anonymous. “Lowering Costs via Voice Over IP.” Government Computer News. Accessed 23 September 2004 <www.gcn.com/research_results/netcomm2.html>.

Anonymous. “The MegaCall QuickStart Guide: Version 2.5.” TelSoft Solutions, Inc. 2000.

Anonymous. “TelSoft Solutions MegaCall Pre-Installation Questionnaire Ver 3.0.” TelSoft Solutions, Inc.

Anonymous. “Voice Over IP Depolyments.” Working Council for Chief Information Officers. <www.cio.executiveboard. com> April 2002.

Arkin, Ofir. “The Trivial Cisco IP Phones Compromise.” Sys-Security Group Whitepaper. September 2002. Accessed 16 June 2004 <www.syssecurity.com/archive/papers/The_Trivial_Cisco_IP_Phones_compromise.pdf>.

Audin, Gary. “Ensuring Reliable IP Telephony in Branch Office Environments.” Integrated Research Whitepaper.

Bingham, Brian J., Paul Strauss and Morris Edwards. "Validating the Business Benefits of Converged Communications." IDC Whitepaper. June 2003.

Brewin, Bob. "Voice over IP coming to NMCI." Federal Computer Week. 4 October 2004. Accessed 2 November 2004 <www.fcw.com>.

Brewin, Bob and Frank Tiboni. "DISA: Shift communications to IP." Federal Computer Week. 6 September 2004. Accessed 2 November 2004 <www.fcw.com>.

Broersma, Matthew. "Experts Warn of VoIP Security Flaws." Techworld.com. 9 June 2004. Accessed 14 June 2004 <www.pcworld.com/news/article/0,aid,116453,00.asp>.

Brunk, Matt. "Troubleshooting IP-PBX Systems: Live And Learn." Business Communications Review. April (2003), 24-30.

Brunner, Stefan and Akhlaq A. Ali. "Voice Over IP 101: Understanding VoIP Networks." Juniper Networks Whitepaper. August 2004.

Buddenberg, Rex. "Information Security." Class Notes dated Feb 2002. <web1.nps.navy.mil/~budden/lecture.notes/infosec/infosec_notes.html>

Buddenberg, Rex. "Quality of Service -- QoS." Class Notes dated Mar 2003. <web1.nps.navy.mil/~budden/lecture.notes/qos_notes.html>

Conroy-Murray, Andrew. "Emerging Technology: Security and Voice over IP – Let's Talk." NetworkMagazine.com. 4 November 2002. Accessed 14 June 2004 <www.networkmagazine.com/article/NMG20021104S0004>.

Duffy, Jim. "Coalition forms to steer VoIP policy." The Edge. 23 Feb 2004. Accessed 14 June 2004 <www.nwfusion.com/edge/news/2004/0223voip.html>.

Durkin, James F. Voice-Enabling the Data Network: H.323, MGCP, SIP, QoS, SLAs, and Security. Indianapolis: Cisco Press, 2003.

Estes, Tom. “Converging Technologies to Meet Headquarters Increasing Communications Requirements.” PowerPoint Slideshow and Brief. 22 June 2004.

Harte, Lawrence. “Introduction to IP Telephony: Why and How Companies are Upgrading Private Telephone Systems to use VoIP Services.” Excerpted From: Voice Over Date Networks For Managers. Althos Publishing: 2005.

Joch, Alan. “VOIP’s second act.” 19 July 2004. FCW.com. Accessed 23 September 2004 <www.fcw.com/fcw/articles/2004/0719/feat-voip-07-19-04.asp>.

Knoll, James A. “Convergence of the Naval Information Infrastructure.” Master Thesis. Naval Postgraduate School, June 2004.

Korzeniowski, Paul. “VoIP Looms Large, But Problems Persist.” TechNewsWorld.com. 28 September 2004. Accessed 30 September 2004 <www.technewsworld.com/story/36938.com.>

Krejci, Joe. Personal Interview. 16 December 2004.

Lazar, Irwin. “Implementing Enterprise Voice over IP.” Burton Group Network Methodologies and Best Practices. <www.burtongroup.com> 2004.

Lazar, Irwin. “Public IP Telephony Services: Leveraging the “IP” in VoIP.” Burton Group In-Depth Research Report. <www.burtongroup.com> 7 September 2004.

Lewis, Rosemary. “Operational Benefit of Implementing VoIP in a Tactical Environment.” Master Thesis. Naval Postgraduate School, June 2003.

LightPointe. “Free-Space Optics: Transmission Security.” LightPointe Whitepaper. 2002.

Louderback, Jim. “Security Holes Make VOIP a Risky Business.” eWeek.com. 12 May 2004. Accessed 10 December 2004 <www.eweek.com/print_article2/0,2533,a=126940,00.asp>.

McCool, Jim. Personal Interviews. 16 December 2004. 17 March 2005.

Mier, Edwin, Randall Birdsall and Rodney Thayer. “Breaking through IP telephony.” Network World Lab Alliance Network World. 24 May 2004. Accessed 26 May 2004 <www.nwfusion.com/reviews/2004/0524voipsecurity.html>.

Muraskin, Ellen. “A Pioneer’s View of VOIP and SIP Security.” eWeek.com. 17 May 2004. Accessed 10 December 2004 <www.eweek.com/print_article2/0,2533,a=127276,00.asp>.

Myser, Michael. “New VOIP Exploits Coming Soon.” eWeek.com. 1 Dec 2004. Accessed 10 December 2004 <www.eweek.com/print_article2/0,2533,a=140212,00.asp>.

Packeteer. “7 Steps to WAN Optimization.” Packeteer Brochure. 2004.

Packeteer. “Is Your Network Ready for VoIP? Tough Questions, Honest Answers.” Packeteer, Inc Whitepaper. 2002.

Passmore, David. “NAT Traversal by Peer-to-Peer Applications: Addressing Variable Behaviors.” Burton Group Network and Telecom Strategies In-Depth Research Overview. <www.burtongroup.com> November 2004.

Passmore, David. “VOIP Regulation For Dummies.” Business Communications Review. Burton Group: 1 September 2004.

Darley, L. Perry. Personal Interviews. 15-17 December 2004. 16 March 2005.

Peterson, Shane. “Buying into VoIP: With the right preparation, VoIP doesn’t have to be a trip to uncharted waters.” Government Technology (govtech.net). October 2003. Accessed 23 September 2004 <www.govtech.net/magazine/story.print.php?id=72709>.

Qovia. “Network Intrusion and QoS impact within VoIP.” Qovia, Inc Whitepaper. 5 August 2004.

Qovia. “VoIP Problem Detection and Isolation.” Qovia, Inc Whitepaper. 25 November 2003. <www.qovia.com/resources/PDFs/white%20papers/voip_problem_final.pdf>.

Rendon, Jim. “The Security Risks of VOIP.” Security Wire Perspectives. Information Security. 6.95 (13 December 2004).

Roberts, Dave. “Defense in Depth for VoIP Networks.” TechNewsWorld.com. 13 September 2004. Accessed 30 September 2004 <www.technewsworld.com/story/36543.html>.

Shim, Choon, Liehue Xie, Bryan Zhang and C.J. Sloan. “How Delay and Packet Loss Impact Voice Quality in VoIP. Qovia, Inc. Whitepaper. 9 December 2003. <www.qovia.com/resources/PDFs/white%20papers/How%20Delay%20and%20Packet%20Loss%20Impact%20Voice%20Quality%20in%20VoIP.pdf>.

Tanase, Matthew. “Voice over IP Security.” SecurityFocus.com. 12 March 2004. Accessed 13 May 2004 <www.securityfocus.com/ infocus/1767>.

Tasymruk, Lutfullah. “Analysis of Voice Quality Problems of Voice Over Internet Protocol (VOIP).” Masters Thesis. Naval Postgraduate School, September 2003.

United States Coast Guard. “COMDTINST M2000.3C: Telecommunications Manual.” 7 September 1999.

United States Coast Guard. “COMDTINST M4000.2: U.S. Coast Guard Logistics Handbook.” 20 March 2001.

United States Coast Guard. “COMDTINST M4200.19H: Coast Guard Acquisition Procedures (CGAP).” 13 October 2004.

United States Coast Guard. “COMDTINST M5200.16: Standard Workstation III Configuration Management Policy.” 24 March 1999.

United States Coast Guard. “COMDTINST 5230.66, Coast Guard Command, Control, Communications, Computers, and Information Technology (C4&IT) Systems Development Life Cycle (SDLC) Policy.” 26 October 2004.

United States Coast Guard. “COMDTINST 5230.67, Coast Guard Command, Control, Communications, Computers, and Information Technology (C4&IT) Information Assurance (IA) Policy.” 30 August 2004.

United States Coast Guard. “COMDTINST 5230.69, Coast Guard Command, Control, Communications, Computers, and Information Technology (C4&IT) Configuration Management (CM) Policy.” 26 October 2004.

United States Coast Guard. “COMDTINST 5230.71, Coast Guard Command, Control, Communications, Computers, and Information Technology (C4&IT) Investment Management Policy.” 11 February 2005.

USCG Headquarters Support Command Telecom Special Projects Team. “U.S. Coast Guard Headquarters 1900 Half Street – Jemal Building Telecommunication Expansion.” 27 September 2004.

Vegter, Henry M. Jr. and David T. Wallace. “Exploitation of Existing Voice Over Internet Protocol Technology for Department of the Navy Application.” Masters Thesis. Naval Postgraduate School, September 2002.

Whiteman, Kip. Personal Interviews. 15-17 December 2004.

Yedweb, David H. “An 11-step program for enterprise VoIP implementation.” <u>TelephonyOnline.com</u>. 14 May 2004. Accessed 1 August 2004 <telephonyonline.com/ar/telecom_step_program_enterprise/index.htm>.

Young, Ray. “Differentiated Services – One Solution for Priority Over the Internet.” <u>Office of the Manager National Communications System Technical Notes</u> 7.1 (April 200).

Zeadally, S, F. Siddiqui and P. Kubher. “Voice over IP in Intranet and Internet Environments.” <u>IEE Proceedings</u> 151.3 (June 2004): 263-269.

# APPENDIX A: INTERNET PROTOCOL TELEPHONY (IPT) SECURITY POLICY RECOMMENDATIONS

## TABLE OF CONTENTS

# CHAPTER 1 INTRODUCTION

## A. BACKGROUND AND PURPOSE

1. Internet Protocol Telephony (IPT) is a rapidly growing and evolving technology that promises to provide enhanced business processes through advanced telephony features and the convergence of voice and data networks. The interaction of voice and data networks introduces security vulnerabilities that can potentially put information systems at risk. The study and implementation of security mechanisms and risk analyses are required to ensure a secure information sharing environment.

2. This document provides a basic overview of IPT and makes recommendations for information security policy guidance, procedures, and processes for implementation of IPT at units in the United States Coast Guard (CG). It is a tool intended to promote the secure deployment and maintenance of IPT-based networks.

## B. AUDIENCE AND SCOPE

1. The target audience for this document includes managers who intend to deploy IPT at their units, information technology personnel, and network and security administrators.

2. It is assumed that the personnel reading this document have a basic understanding of traditional telephony, operating systems, network operation, and data network security. This document addresses security issues that are unique to or particularly important for IPT-based networks and their components. It applies to all IPT systems and devices within the CG's information infrastructure and operating environment.

3. These recommendations are intended to complement other CG Information Technology and Security Policy, including:

    a. *Policy on Coast Guard use of Internet/Worldwide Web*, COMDTINST 5230.56.

    b. *Coast Guard Limited Personal Use of Government Office Equipment*, COMDTINST 5375.1A (series).

    c. *Coast Guard Physical Security and Force Protection Program*, COMDTINST M5530.1 (series).

    d. *Coast Guard Information Assurance Manual*, COMDTINST M5500.13 (series).

e. *Coast Guard Command, Control, Communications, Computers, and Information Technology (C4&IT) Information Assurance (IA) Policy*, COMDTINST 5230.67.

f. *Coast Guard Telecommunications Manual*, COMDTINST M2000.3 (series).

4. The following documents also provide useful recommendations to understand and deploy secure IPT-based networks:

   a. Defense Information Systems Agency (DISA) *Voice Over Internet Protocol (VOIP) Security Technical Implementation Guide*

   b. *Security Considerations for Voice Over IP Systems: Recommendations of the National Institute of Standards and Technology (NIST),* Special Publication 800-58

5. The rapidly evolving nature of the IPT environment requires that security policies and practices be reviewed frequently to adequately adjust to changes. IPT policy should be updated at least annually until the technology settles.

## C. INTERNET PROTOCOL TELEPHONY (IPT) DEFINITION

1. A variety of terminology has been coined to describe the process of replicating the function of the Public Switched Telephone Network (PSTN) by moving voice on data networks, including: Voice over Internet Protocol (VoIP or VOIP), Internet telephony, internet telephony, Voice on the Net (VON), next-generation telephony, computer telephony, packet telephony, intranet telephony, extranet telephony, etc. For the purpose of this document, Internet Protocol Telephony encompasses these terms and refers to the components and technology required to place telephone calls over any IP-based network; that is, transferring voice data over a packet-switched network.

## D. DOCUMENT ORGANIZATION

1. Chapter 1 provides the background and definition of IPT and the purpose, audience, scope, and organization of the document.

2. Chapter 2 briefly discusses an overview of the operation of and the equipment used for IPT-based networks, to include: Components, Protocols, Voice Quality, and Architectures.

3. Chapter 3 outlines potential threats to and vulnerabilities of IPT and presents various consequences of a successful attack.

4. Chapter 4 presents the mechanisms used to secure an IPT-based network, mitigating the risks mentioned in Chapter 3. Security measures discussed include: policy, physical security, logical separation, traffic management, hardening IPT equipment, encryption, authentication, and redundancy.

# CHAPTER 2 INTERNET PROTOCOL TELEPHONY (IPT) OVERVIEW

## A. INTRODUCTION

1. To understand how voice data moves across packet-switched networks to make IPT phone calls, this chapter provides a description of equipment and protocols that make up an IPT-based network and allow it to communicate with other networks like the PSTN. The system elements described are useful points to identify potential vulnerabilities.

2. Applying security mechanisms to IPT-based networks often comes at a cost of reduced call quality. To understand how security affects quality, this section describes how voice quality is measured and influenced.

## B. COMPONENTS

1. **Telephones**: IPT phones can take many forms. They sometimes use a *traditional handset* that is connected to an adapter that utilizes bandwidth provided by an internet service provider (ISP). They may exist in the form of *Softphones*, where a PC with a microphone and software are used to create a virtual phone. The most common IPT telephone, called an *IP Phone*, consists of a handset and a processor that provides varying degrees of IPT functionality depending on the model.

2. **IP network**: The network that IPT packets traverse is made up of similar components as the standard data network. Hubs and Switches logically connect many nodes together, Routers connect networks, and Servers provide most of the intelligence. These components are linked with a variety of media, like, copper wire, fiber optic cable, wireless, satellite, etc.

3. **Call Processors/Controllers**: These devices set up, monitor, and tear-down calls. They can coordinate signaling, address translation, access control, bandwidth use, and call features. They are sometimes called gatekeepers, call agents, call managers, or softswitches depending on how they are used.

4. **Gateways**: Gateways connect dissimilar networks, protocols, or formats. For instance, they may be used to connect an IPT-based network to the PSTN or to convert analog voice signals to digital data packets. There are three basic types of gateways:

   a. *Media Gateway (MG)*: The media gateway coordinates the transfer of data between different networks by, for example, providing an interface between a packet switched network (e.g., IPT) and a circuit switched network (e.g., PSTN).

   b. *Signaling Gateway (SG)*: The signaling gateway coordinates the signaling functions between two networks by, for example, connecting the IP network to signaling system seven (SS7) of the PSTN.

c. *Media Gateway Controllers (MGC)*: The media gateway controller coordinates the roles of the MG and the SG so that signaling and data transport functions can work together to complete a call.

## C. PROTOCOLS

1. Many standards and protocols are used to exchange voice information between different systems and devices. Some of the most commonly used IPT protocols will be briefly discussed. They can be split up into two general groups: transport protocols that move the data of interest (i.e., voice) and signaling protocols that set up the connection.

2. Transport protocols consist of well known protocols like the *Transmission Control Protocol* (TCP), the *User Datagram Protocol* (UDP), and *Real-Time Transport Protocol* (RTP).

   a. **TCP** is a connection orientated protocol ensures reliable information exchange by acknowledging receipt of packets and resending unaccounted for packets. This process works well for transferring data like email, but for real-time applications like voice conversations. However, TCP is often used to carry higher-layer protocols that setup and tear down IPT calls.

   b. **UDP** is a connectionless orientated protocol, is simpler than TCP and is used where reliable transmission of every packet is not critical. UDP has much less overhead and does nothing to acknowledge or resend packets. Though packets may be lost, it is usually acceptable since a single lost packet does not significantly effect the transmission of information

   c. **RTP** is a higher-layer protocol that is encapsulated in UDP and is specifically used to support streaming real-time multimedia applications like IPT. RTP carries the bulk of the voice conversation between two IPT endpoints once a connection is established.

3. Signaling protocols set up and manage telephone calls in the IPT-based network. The two most widely accepted standards today are *H.323* and *Session Initiation Protocol* (SIP), while a variety of other proprietary protocols are also in use. The *MEdia GAteway COntrol(MEGACO)/H.248* standard that allows communications between diverse networks will also be discussed.

   a. **H.323**: The H.323 standard, developed by the International Telecommunication Union (ITU), encompasses a set of standards designed to enable real-time multimedia (voice, video, and data) communications over a packet-switched network. H.323 is described by four primary components: terminals (telephone), gateways, gatekeepers, and Multipoint Control Units (which provides conferencing). This is one of the first protocols developed for IPT and is currently the most widely supported. The high level of detail of the standard provides for excellent interoperability but has high overhead and is slow to change.

b. **SIP**: Session Initiation Protocol (SIP) was standardized by the Internet Engineering Task Force (IETF) in 1999 as Request for Comment (RFC) 2543. SIP-based networks consist of two main components, User Agents and Servers. *User Agents* (UA) are endpoints (e.g., IP telephones) that contain a Client (*UAC*) and a Server (*UAS*). The UAC initiates requests and the UAS responds to requests. There are several SIP servers that provide services on the IPT-based network. *Proxy servers* make requests in behalf of other clients, *Redirect servers* provide address translation, *Register servers* register clients on the network, and *Location servers* provide the call recipient's possible location to other servers. SIP components are identified with Uniform Resource Locators (URL) to simplify addressing. The protocol was designed with simplicity in mind, focusing on session initiation and termination, while relying on other Internet Protocols (such as TCP, UDP, and RTP) to complete the process. SIP is much like HTTP, using text-based messages to setup call connections. This "lightweight" protocol is expected to dominate the industry because it facilitates quick, scalable IPT solutions and creates the potential for a variety of features that the PSTN or H.323 are too slow to provide.

c. *Proprietary Protocols*: These are standards that have been created by commercial organizations to support IPT (e.g., Cisco's Skinny Client Control Protocol). Proprietary protocols generally do not interoperate with other standards and should be avoided to provide the most flexible network.

d. **MEGACO/H.248**: This standard was developed jointly by the ITU and IETF and complements SIP and H.323 in order to connect dissimilar networks. It refers to MGCs as *Call Agents* and has different gateways that provide interfaces between IP networks and a variety of other networks. For instance, "*trunking gateways*" manage many digital circuits to connect the PSTN to an IPT-based network, "*business gateways*" connect PBXs to IPT-based networks, and "*residential gateways*" provide an analog connection to the IP network via cable modems and other devices.

## D. Voice Quality

1. Measuring Quality: The most widely accepted method of evaluating voice quality is a subjective assessment called the mean opinion score or MOS. MOS is calculated by having several human listeners rate the quality of a call on a scale of 1 to 5 and taking the average. Several algorithms have been created to estimate voice quality and map their scores to the MOS model. A MOS of 4 or higher is considered toll quality, while a value less than 3.6 usually causes dissatisfaction.

2. Reductions in voice quality are most commonly caused by latency, jitter, and lost packets. *Latency* or delay is the amount of time it takes for voice to travel from the speaker's mouth to the receiver's ear. *Jitter* refers to variations in the arrival time and order of packets. Jitter can potentially cause packets to be assembled out of sequence or to be dropped. *Lost packets* are those packets that are dropped in

the network, whether from improper routing, corrupted data, overflowing queues, or late arrivals.

3. Other factors that affect quality are echo, available bandwidth, voice activity detection (VAD), and codec selection. *Echo* is created when the receiver's telephony equipment amplifies and returns parts of the original signal back to the sender. *Bandwidth* is the amount of information that can pass through a medium at one time. The larger the "pipe", the more data that flows through it. When bandwidth is low, information flow slows down and reduces quality. *VAD* sends smaller data packets during breaks in conversation to conserve bandwidth, but sometimes cuts off the beginning of phrases. *Codecs* convert between analog and digital signals, and compress and decompress signals. These processes add delay and sometimes lose information to conserve bandwidth.

4. *Quality of service (QoS)*: QoS refers to services that give priority to certain packets, such as time-sensitive IPT packets over web browser traffic, to improve the affects of packet loss, jitter and delay. A variety of protocols are in use or being planned to help prioritize real-time data flows. They give priority to packets from time sensitive applications like IPT, subsequently slowing the processing of other information flows where time is less critical (like email). The use of QoS mechanisms is considered a must to successfully attain good call quality on data networks.

## E. ARCHITECTURES

1. There are several IPT-based network designs that provide varying levels of IPT capability and network control to an organization. The following four are considered:

    a. *Broadband services*: These are services that are typically used by residential customers to save on long distance phone calls. They rely on a users existing broadband connection to provide service over the Internet. Services vary. For instance, among other services Vonage supplies its users with Analog Telephony Adapters that allow them to connect their traditional phones to their home routers. Other services, like Skype, are peer-to-peer services that require common (free) software between two users.

    b. *IP-PBX*: The Internet Protocol Private Branch Exchange (IP-PBX) is used by agencies to enable many features of an IPT-based network. It is usually located within and owned by an organization. It provides services for many users with fewer resources by sharing lines (but not phone numbers). Further savings and functionality are achieved by connecting IP-PBXs at different offices. It is connected to the PSTN through a dedicated trunk.

    c. *IP-enabled PBX*: This is a hybrid solution, where a circuit-switched PBX is provided with interfaces for IPT equipment. It allows an incremental introduction of IPT without losing the features of the current PBX.

d. *IP Centrex*: A local service provider supplies the core IPT services for those organizations that wish to save costs on equipment and space. The disadvantage to this approach is that fewer features are available and businesses have less control of the network, making it more difficult to make changes or protect information.

# CHAPTER 3 IPT SECURITY RISKS

## A. INTRODUCTION

1. Common IPT-based network threats, vulnerabilities, and attacks must be recognized to understand and implement appropriate security countermeasures.

## B. THREATS

1. Security threats are those actors that attack or interact with data networks to degrade system security.

2. IPT-based networks are exposed to the same information threats (internal, criminal, and foreign) that are described in section 2.G of the CG's Information Assurance Manual (IAM).

3. Network administrators should also be familiar with "Phreakers," criminal hackers who attempt to make free phone calls (Toll-fraud) at the CG's expense.

## C. VULNERABILITIES

1. Vulnerabilities are weaknesses in IPT-based networks that potentially enable system exploits. This section enumerates several elements of IPT-based networks that make them vulnerable.

2. *Network Convergence*: When combining the data and voice networks, the telephony elements may become affected by the known (and unknown) vulnerabilities of the data network, and vice versa. This convergence also brings the signaling and data transport components of telephony together onto a common system, which are distinct on the PSTN. The generally isolated PSTN, with its separation of signaling and voice transport networks, is generally thought to provide a more secure environment.

3. *IPT Protocols*: IPT relies on internet protocols (e.g., TCP/IP, UDP, RTP, etc.) to perform signaling and transport data. The security risks inherent in these supporting protocols transfer into the IPT domain. Furthermore, many have observed that internet protocols are often designed with functionality first and security mechanisms later; including IPT protocols like SIP. Also, security mechanisms like firewalls and network address translation (NAT) are more difficult to implement with IPT protocols.

4. *Placement of Intelligence*: More processing and configuration occurs at the endpoints (i.e., telephones) on IPT networks than on traditional telephone systems. This requires increased protection of simple telephony devices.

5. *IPT Components*: Any piece of equipment in the IPT-based network can become the target of an attack, especially those that have a logical connection to the data

network. IPT Servers, gateways, network interfaces, and endpoints require special attention to ensure appropriate security mechanisms are in place.

6. *Availability*: Network congestion and outages are common on data networks and are tolerated to a certain degree; however, an IPT-based network must be more reliable. An attack directed at shutting down or slowing the data network will disrupt telephone service and slow accomplishment of unit objectives.

## D. ATTACKS AND CONSEQUENCES

1. This section lists common methods of exploiting vulnerabilities and the impact of successful attacks.  It will focus on attacks that are common to both the IPT-based network and data network, and on attacks that are unique to the IPT environment.

2. *IPT Phone Service Disruption*: This is an attack on availability.  Degraded availability in this case can refer to poor voice quality, the inability to connect with or receive calls from a desired party, or complete loss of telephony service.

   a. Availability is compromised through Denial of Service (DoS) and Distributed DoS attacks that are enabled by viruses and worms.

   b. Attackers that gain access to equipment by using methods like Trojan horses, buffer overflow attacks and backdoors can affect availability by intercepting calls (call hijacking) or changing system configurations that reduce call quality.

   c. Even “spit” (spam over internet telephony) can affect availability by tying up phone lines or through blocked calls that are filtered out by anti-spam mechanisms.

   d. The damage of these attacks can vary from minor irritations and inconveniences to the interruption of mission critical operations and life threatening situations.

3. *Compromise of Confidentiality*: Confidentiality describes the ability to keep private, confidential, or propriety information secret. IPT vulnerabilities provide opportunities for hackers to eavesdrop on conversations, to track signaling, to monitor billing records, and to see private information.

   a. Hackers can easily extract information from unencrypted packets that pass through sniffing devices under their control. Packets may pass through an attackers sniffer (1) as a necessary consequence of placing calls through untrusted networks like the Internet, (2) as a result of using hubs that broadcast packets to all devices they are connected to, (3) because an attacker physically attached the device to the network (e.g., insider attack), (4) because the attacker gained access to one of the network devices (e.g., buffer overflow or back door), or (5) because the attacker configured a network device to redirect (or send copies of) the packets (e.g., ARP Cache Poisoning).

b. When hackers are unable to determine the content of the messages on the network, they may still learn valuable information by sniffing the network through traffic flow analysis.

c. Hackers are not the only enemies to confidentiality. Complacent employees, usually with no malicious intent, frequently fail to keep calls private. Whether it be speaking loudly amongst a group of cubicles, failing to close a door or window, or chatting on a wireless or cell phone, people often create vulnerabilities that no amount of network security mechanisms will overcome.

d. Failure to maintain confidentiality can lead to such consequences as identity fraud and operational or National Security risks when sensitive information is compromised.

4. *Compromise of Integrity/Authentication*: Integrity describes the ability to recognize if a packet has been altered (whether by mistake or intentionally). Strong integrity demonstrates that the message received is trustworthy and in its original form. Authentication is related, providing the means to reliably identify the source of a message. One step further is non-repudiation, a mechanism that prevents users from denying that they originated the message. When in place, these tools provide confidence in information from a known user on the other end. Hackers subvert these mechanisms in a variety of ways on the data network, but frequently work around them on an IPT-based network through spoofing.

   a. Hackers are able to gain control of endpoints by forcing them to restart (e.g., DoS) and then spoofing the address of the configuration server.

   b. Attackers may use a man-in-the-middle attack to intercept packets and retransmit packets without the sender or receiver's knowledge.

   c. Caller ID is an example of a telephony feature that has been successfully spoofed on IPT-based networks. Hackers have found a way to display any number they want, and can bypass Caller ID blocking to discover the phone number of anonymous numbers.

   d. Complacent or naïve human behavior is often a target of these attacks. Personnel who use default passwords, simple passwords, or become victim to social engineering can expose their systems to unauthorized access and allow malicious parties to act in their behalf.

   e. The consequence of a loss of integrity is the potential to make decisions based on false information.

5. *Toll Fraud*: Phreakers have been trying to get free phone calls from the PSTN for years and continue to pursue the same goal on IPT-based networks. Common methods of acquiring toll free calls consist of: intercepting and rerouting signaling, gaining access to network devices that record call billing, and gaining

access to another individuals IP phone. Simple employee abuse of telephone use, however, can be just as costly.

6. *IPT Components*: The components of the IPT-based network are the focus of attacks, usually to disrupt service or to gain unauthorized access. Hackers will use a combination of many of the attacks already to meet their goals.

    a. Endpoints: The intelligence contained in IP Phones allows much more control of the network. Hackers can gain access to IP Phone configurations by forcing IP phone reboots, spoofing TFTP servers, and breaking passwords. Softphones are particularly vulnerable because they are susceptible to any of the worms, viruses, or operating system/application software bugs that the computer may encounter.

    b. The switches and routers on the network are targeted to disrupt or redirect the flow of traffic on an IPT-network. A hacker will attempt to eavesdrop or intercept phone calls at switches on the network.

    c. The servers in an IPT-based network hold most of the information of value (e.g., billing, address translation, configurations, etc.) and are thus a prime target. Hackers attempt to gain control of the servers or disrupt the network by bringing them down. A server that is compromised usually leads to a compromise of the entire IPT-based network.

    d. Gateways: The complexity of interfacing dissimilar networks provides great opportunity for hackers to identify bugs or to use known vulnerabilities of either network. They can subsequently exploit those bugs with the potential of gaining control over components of two networks, a vulnerability that was less common to the PSTN prior to the emergence of telephony over packet-switched networks.

# CHAPTER 4 IPT SECURITY MEASURES

## A. INTRODUCTION

1. IPT-based networks inherit many of the same vulnerabilities that already exist on the data network; therefore, many of the same security mechanisms that are used for the data network can be applied. However, the real-time nature of IPT often limits the use of certain safeguards because of their effect on voice quality. This chapter presents recommended standards, guidelines, and procedures that should be followed to secure the IPT-based network. These standards are intended to complement and be used alongside (not replace) the data network security guidance provided in the CG IAM.

## B. GENERAL POLICY CONSIDERATIONS

1. This policy shall be reviewed and updated at least annually to adapt to the rapidly evolving IPT environment.

2. Policy is only effective when practiced. The following steps shall be taken, along with measures outline in section 4.J of the CG IAM, to encourage compliance:

    a. Provide appropriate training (e.g., rules of behavior, security awareness, acceptable security practices, etc.) to personnel as required by section 3.J and chapter 5 of the CG IAM and make policy documentation readily available.

    b. Actively enforce policy by holding personnel accountable for ignoring mandated standards and procedures.

    c. When possible, automate policy in information technology systems and confirm its accuracy regularly.

3. Prior to implementation, conduct an evaluation of the unit's ability to manage and mitigate the risks to its information, system operations, and continuity of essential operations when deploying IPT systems. The implementation guide presented with this document will facilitate this process.

4. When designing, implementing, and maintaining IPT security models, the following general policy from section 2.H of the CG IAM must be considered:

    a. All IT that generates, stores, processes, transfers, or communicates information shall be protected at a level commensurate with the threat.

    b. System planners, organizational managers, and users (e.g., system administrators and end users) will have a common understanding of Information Assurance principles, concepts, and interrelationships.

    c. The threat to the CG's information is measured by the capability and intention of an adversary.

d. All CG Information Systems shall be certified and accredited for officials appointed Designated Accrediting Authorities (DAA). Certification and accreditation shall be performed before the system is placed into operation. Systems and applications shall be reaccredited whenever there is a major change, or every three years, whichever occurs first.

e. The Information System shall meet or exceed minimum security countermeasures as required by federal and departmental security policies, standards, procedures and CG policies. All CG information and information resources shall be appropriately safeguarded at all times in order to support a defense in depth, or layered, information assurance policy.

5. IPT shall not be the primary voice communications system if the information it carries is considered to be Mission Critical, Category 1 as defined in section 2.J in the CG IAM.

6. In accordance with COMDTINST 5375.1, Limited Personal Use of Government Office Equipment, the use of peer-to-peer broadband IPT services (e.g., Skype) shall not be used because they must circumvent or weaken security mechanisms to operate correctly.

7. To reinforce the safety of human resources, Emergency 911 location services must be included in the unit's telephony system, whether it be through the PSTN or via IPT.

## C. PHYSICAL SECURITY

1. Due to the vulnerability and potential consequences of compromised IPT network equipment, physical access to all IPT equipment must be closely monitored and limited to authorized personnel only. Ensure that physical countermeasures are in place to mitigate the risk of insertion of sniffers or other network monitoring devices.

2. All unclassified IPT equipment, except for endpoints and cabling, shall be considered Sensitive/Critical Information Systems (SCIS) and protected in accordance with Chapter 2 of the CG Physical Security and Force Protection Program (PS & FPP). Endpoints shall be considered Non-Critical Information Systems (NIS) and protected accordingly. Cabling exposure to open areas must be limited as much as possible.

3. Prepare controls for unexpected occurrences like fire, flooding, natural disasters and other acts of nature:

   a. Develop a disaster recovery plan and test it annually.

   b. Install a Heating, Ventilation, and Air Conditioning (HVAC) unit appropriate to the facility that houses network equipment. This prevents overheating and the potential of damage caused by static electricity.

4. Support physical security by keeping configuration information and system documents (e.g., network diagrams) out of plain view, by using installed locks, and by physically disconnecting all unused ports and disk drives.

5. Escort and log visitors in restricted areas in accordance with section 5.G.3 of the IAM and Chapter 2 of the CG PS & FPP.

6. Monitor the use of portable electronic devices (PEDs) in restricted areas in accordance with Chapter 4 of the CG PS & FPP.

## D. Logical Separation

1. To isolate the IPT network from the data network, logically separate the IPT network from the data network by putting them on different virtual local area networks (VLANs). Wireless devices and Softphones should also be on separate VLANs. Logical separation reduces the risk of IPT network exposure to data network attacks and improves performance. However, if a device handles both voice and data networks, the IPT functionality will falter if the device shuts down due to a data network attack.

2. If possible, replace all hubs on the IPT network with switches. Hubs broadcast packets to all devices they are connected to and cannot logically separate data flows.

3. Disable all VLAN ports that are not in use, including all data network ports on IP phones.

4. Where possible, use Network Address Translation (NAT) and the Private IP Address space to mask internal addresses from external users and to separate IP telephony from the data network where interaction is required. Use caution when implementing NAT, since its use can conflict with other security mechanisms or prevent phone connections.

5. IP phones must be VLAN capable and assigned to an IPT VLAN segment. Softphones must have a separate dedicated NIC for IPT VLAN access.

6. If wireless IP phones are utilized, use products implementing WiFi Protected Access (WPA), rather than 802.11 Wired Equivalent Privacy (WEP). However, neither standard fulfills the Federal Information Processing Standard (FIPS) 140-2 standard for information that must be encrypted. Other protocols such as secure shell (SSH), Transport Level Security (TLS) or Internet Protocol Security (IPsec) shall be used for encryption on wireless networks. Adhere to the guidance provided in the CG IAM and CG PS & FPP for wireless applications.

## E. Manage Network Traffic

1. Firewalls, Intrusion Detection Systems (IDS), and NAT traversal mechanisms must be used at network boundaries to provide protection from external threats.

Careful planning is required to ensure these devices are deployed in the right places with functionality appropriate to the needs of the network.

2. Firewalls are essential network security tools that are used to block undesirable traffic, both entering and leaving the network. However, they form bottlenecks that add delay to the system, significantly impacting the quality of IPT communications. Therefore, IPT firewalls must be stateful and specifically designed for IPT applications in order to process IPT packets that would otherwise be blocked or delayed.

3. At a minimum, Stateful Firewall Filtering that supports required IPT protocols (e.g., SIP, H.323) shall be implemented between the IPT network and the data network at critical IPT servers.

4. An IPT Firewall dedicated to IPT traffic shall be deployed at the security perimeter to support voice quality by reducing delay.

5. A restrictive firewall policy shall be applied, where all packets are initially denied and only necessary ports are opened to allow traffic.

6. Remote administration and configuration of firewalls may only occur through encryption or tunneling via a Virtual Private Network (VPN) (e.g., IPsec). Other methods of remotely accessing Firewall configurations shall be blocked at the perimeter.

7. Test firewall configurations, particularly IPT traffic filtering, at least quarterly.

8. Adhere to other firewall guidelines in accordance with section 6.C.4 of the CG IAM.

9. Place at least one Network-based Intrusion Detection System (NIDS) at the edge of the IPT network perimeter where it can observe traffic that flows in and out of the data network. Carefully determine a configuration that will promptly alert human resources to suspicious activity or that will block malicious traffic. NIDS must be carefully tuned to avoid either blocking legitimate traffic or allowing malicious packets into the network.

## F. HARDEN IPT EQUIPMENT

1. IPT-based network equipment must be secured to prevent hackers from gaining control of critical network devices. Call servers, mail servers, and other IPT-based network servers hold sensitive data and perform critical functions that require special defenses. These servers must be dedicated to only applications required for IPT operations. A suggested method to harden servers follows, use the CG IAM and other CG security policy to assure servers are adequately protected:

   a. Install the operating system on a clean hard drive.

b. Apply the latest patches. Subscribe to a service that will provide continuous updates on new patches.

c. Run a vulnerability assessment tool and take steps to mitigate identified vulnerabilities.

d. Install a firewall on the server computer. Start with a restrictive policy (don't allow any traffic) and then open only those ports required to serve its function.

e. Consider Installing a Host-based IDS.

f. Install antivirus software and ensure it is up to date. Utilize automatic update functionality that will automatically check for updates and download them.

g. Create an Image after following the steps above and use it to create other IPT servers.

h. Change default configurations to match security policy. This can be done using software. Adjust the boot sequence to prevent hackers from gaining access by forcing a system crash and reboot. Be sure default passwords are changed.

i. Turn off or disable all unnecessary services and applications that are not in use. This may include disk drives and physical ports. Each service is a potential avenue of attack for a hacker.

j. Avoid the use of shared drives.

2. Voice Mail Servers require special security when they provide unified mail, because it introduces a point where the data network and IPT network must be logically connected.

   a. A stateful firewall shall be installed between the voice VLAN and the data network to deny all traffic that is not necessary for voice calls or voice messages to be transferred between the voice VLAN and the data network if the voice mail platform is connected to the data network.

   b. The Voice Mail Server and Applications shall be hardened as described above.

   c. Personal voice mail settings may only be changed via a Secure Socket Layer (SSL) connection to ensure authentication. HTTP and Telnet services shall be disabled.

3. Harden IP Phones by updating passwords, by requiring authentication, by disabling unnecessary ports and services, by updating reboot sequences, and by disabling automatic registration mechanisms.  Treat public IP Phones differently by limiting available features and services.

4. Prefer IP Phones to Softphones. Softphones are located on data network devices (PCs) and are vulnerable to the worms, viruses, and other attacks prevalent among personal computers. Do not count on privacy or security when using Softphones.

5. The installation and use of personal Softphone agent software is prohibited. Only IP Softphone agent software approved by the DAA may be used. This policy must be closely monitored and constantly enforced to protect the security of the IPT network.

## G. ENCRYPT AND AUTHENTICATE IPT TRAFFIC

1. Encryption of IPT packets requires special consideration because of the negative effect it can have on call quality. Careful selection of IPT equipment and encryption standards are required to facilitate both confidentiality and good call quality. End-to-end encryption protects a voice conversation from the caller's telephone to the callee's telephone; however, its use is not required for all calls because IP Phones on both ends frequently do not have encryption mechanisms or adequate processing speed to assure quality. Link-level encryption may be used via VPN technology or more efficient gateway devices to protect the confidentiality of voice conversations.

2. All IPT traffic that traverses the public Internet shall be encrypted according to the standards specified in section 6.D of the CG IAM.

3. The use of IP Security (IPsec) shall be considered to provide for security functions, authentication, and encryption of IPT-related traffic.

4. All remote administrative connections to critical IPT servers and other IPT equipment shall be encrypted using IPsec, SSH, or other encryption or tunneling mechanisms. When possible, avoid remote administration and access IPT components from a physically secure location.

5. Identify and Authenticate users in accordance with section 6.B of the CG IAM.

## H. REDUNDANCY

1. To approach the level of reliability usually provided by the traditional telephone network, an IPT-based network must have several redundant systems in place to overcome downtimes that are relatively common among data networks. Redundancy and planning also ensures telephone operations when disaster strikes.

2. Data must be protected by making regular backups of critical systems. They should be created in reliable memory systems and stored in a secured, offsite location.

3. The network must be protected using a layered strategy or "Defense in Depth." This describes the use of several security mechanisms that complement each other

and overlap, rather than a reliance on a single defense. Compliance with the CG IAM will facilitate a layered strategy.

4. Use configuration management tools to proactively track changes to the IPT system. Be prepared to fall back on previous versions when newly installed software, equipment, or configurations weaken security mechanisms.

5. The operation of critical equipment is assured by providing redundant systems that are ready to go online when the current systems fail. All equipment must be protected from power fluctuations and power loss with surge protectors and Universal Power Sources to allow controlled shutdowns. Critical systems shall be backed up with generator power.

6. The IPT-based network shall be supported by out-of-band communications, usually the PSTN. Secondary communications provide an improved likelihood of successful communications when confronted with high call volumes, emergencies, attacks on the data network, or failure of the IPT network.

7. Disaster Recovery Planning (and practice), as mandated in section 5.O of the CG IAM, shall include the IPT-based network.

THIS PAGE INTENTIONALLY LEFT BLANK

# APPENDIX B: INTERNET PROTOCOL TELEPHONY (IPT) IMPLEMENTATION GUIDE

## TABLE OF CONTENTS

# CHAPTER 1 INTRODUCTION

## A. Background and Purpose

1. Internet Protocol Telephony (IPT) is a rapidly growing and evolving technology that promises to provide enhanced business processes through advanced telephony features and the convergence of voice and data networks. These benefits come at a risk to security, quality, and reliability of the telephone network. Careful planning is required to implement a telephony solution that supplies improved service, but also effectively mitigates the risks introduced by the new technology.

2. Despite continuous change occurring in the area of IPT, the technology has been in use long enough to develop practices that yield successful IPT deployments. However, there is not a "one size fits all" approach that is appropriate for all organizational entities. The purpose of this document is to outline the important quality attributes of an IPT-based network and provide recommended, adaptable processes that facilitate the achievement of those characteristics in harmony with Coast Guard Policy.

## B. Internet Protocol Telephony (IPT) Definition

3. A variety of terminology has been coined to describe the process of replicating the function of the Public Switched Telephone Network (PSTN) by moving voice on data networks, including: Voice over Internet Protocol (VoIP or VOIP), Internet telephony, internet telephony, Voice on the Net (VON), next-generation telephony, computer telephony, packet telephony, intranet telephony, extranet telephony, etc. For the purpose of this document, Internet Protocol Telephony encompasses these terms and refers to the components and technology required to place telephone calls over any IP-based network; that is, transferring voice data over a packet-switched network.

## C. Suggested References

1. IPT implementation requires study and research beyond the scope of this document, particularly because the technology continues to evolve. Managers must also have an understanding of relevant Coast Guard Policy. This document is a guide to facilitate the consideration of significant requirements, challenges, and solutions that are involved in deploying IPT. The following resources, among others, may be used to help understand and deploy successful and secure IPT-based networks in the Coast Guard environment.

    a. Walker, John Q. and Jeffrey T. Hicks. Taking Charge of Your VoIP Project. Indianapolis: Cisco Press, 2004.

    b. Miller, Mark A. Voice over IP Technologies: Building the Converged Network. New York: M&T Books, 2002.

c. *Coast Guard Command, Control, Communications, Computers, and Information Technology (C4&IT) Systems Development Life Cycle (SDLC) Policy*, COMDTINST 5230.66.

d. *Coast Guard Command, Control, Communications, Computers, and Information Technology (C4&IT) Information Assurance (IA) Policy*, COMDTINST 5230.67.

e. *Coast Guard Command, Control, Communications, Computers, and Information Technology (C4&IT) Configuration Management (CM) Policy*, COMDTINST 5230.69.

f. *Coast Guard Command, Control, Communications, Computers, and Information Technology (C4&IT) Investment Management Policy*, COMDTINST 5230.71.

g. Security Policy Recommendations in Appendix A that is supported by the *Coast Guard Information Assurance Manual*, COMDTINST M5500.13 (series) and the *Coast Guard Physical Security and Force Protection Program*, COMDTINST M5530.1 (series).

h. *Security Considerations for Voice Over IP Systems: Recommendations of the National Institute of Standards and Technology (NIST)*, Special Publication 800-58.

i. Defense Information Systems Agency (DISA) *Voice Over Internet Protocol (VOIP) Security Technical Implementation Guide*.

## D. DOCUMENT ORGANIZATION

1. Chapter 1 provides the background and definition of IPT, suggested reference material, and the purpose and organization of this document.

2. Chapter 2 briefly discusses an overview of the important requirements and quality attributes that must be addressed to effectively implement an IPT-based network. The issues discussed include: Cost, Security, Sound Quality, Resilience, Power and Reach, Network Management, Platform Independence, Support of Legacy Services, Scalability, Features, User Mobility, and Emergency Services.

3. Chapter 3 provides some of the processes, methods, and practices used by successful organizations to support the requirements and quality attributes described in Chapter 2. The overall implementation process described addresses the following steps: Form an Implementation Team, Understand Current Telephony Requirements, Understand Current Data Network Infrastructure, Update the Data Network, Develop the Business Case & Acquire, Create an Implementation Plan, Deployment, Network Management & Maintenance, and Manage Change.

# CHAPTER 2 IPT NETWORK KEY ATTRIBUTES

## A. PURPOSE

1. Several areas of focus that must be considered to realize viable communications using packet-switched networks. Proactively addressing each of these technical and operational issues is a common success factor among organizations that have already attained the benefits of IPT. This chapter enumerates several requirements and quality attributes, of viable IPT-based networks, which must be taken into consideration when designing an IPT solution.

## B. COST

1. The initial push towards IPT was based on the desire to achieve cost savings through free long distance and international calls. Residential users, for instance, still realize savings through IPT services. However, bypassing toll charges is usually not reason enough to switch to IPT services because government agencies are charged very little for services through government wide telecommunications contracts.

2. The total cost of an IPT-based network will depend on the size and scope of the implementation and the equipment required. Large start up costs can hinder IPT development, especially when completely replacing large portions of the telephony infrastructure. However, incremental conversions from aging PSTN equipment to newer IPT technologies are manageable and provide increased value over time.

3. The most convincing argument for cost savings is attributed to the convergence of the voice and data networks. By putting voice and data on the same network, organizations can save on the costs (after initial implementation) of supporting and maintaining one physical network with one support team (vice separate telephony personnel and data network personnel).

4. The cost benefits of IPT discussed present a solid argument for a transition away from the PSTN; however, an IPT-based network may not be the best solution in all cases. It is unwise to invest in technology just for technology's sake. Each unit must carefully consider its options and make an unbiased business case for a particular telephony implementation.

## C. SECURITY

1. An information system must be able to ensure appropriate levels of confidentiality, integrity, availability, authenticity and non-repudiation in accordance with the Coast Guard Information Assurance Manual.

2. Phone conversations need to be private (confidentiality) and trusted (integrity, authenticity, non-repudiation).

3. The telephone system must provide a level of availability that allows for reliable operation, especially when there are emergencies or high call volumes.

4. The personal information (e.g. Names, phone numbers, billing information) that resides in the IPT-based network must be protected from access (confidentiality) or unauthorized modification (integrity).

5. The IPT network has many vulnerabilities that make voice information susceptible to compromise. Network security must be an integral part of any IPT deployment.

6. Implementing security mechanisms frequently comes at a cost of increased bandwidth, equipment upgrades, or degradation in voice quality.

7. It is impossible to eliminate all security risks without rendering the network ineffective or too costly. Therefore, each Coast Guard organization must balance between risk mitigation techniques, cost, and capability of the IPT-based network.

## D. SOUND QUALITY

1. Sound quality and security are often at odds with each other in an IPT-based network. It is very difficult (i.e., expensive) to realize high levels of both quality and security equal to that provided by the PSTN.

2. Quality can be monitored and measured by observing the mean opinion score (MOS), latency, jitter, and lost packets in the IPT-network. These metrics should be understood for varying network conditions (e.g., peak and average call volumes) in different portions of the network.

    a. The MOS is a subjective score of voice quality that is determined by having people listen to conversation over a voice network. A score of 4.0 or greater is considered “toll quality,” while a scores less than 3.6 are considered to have poor (irritating or unacceptable) call quality. The MOS is often estimated by using computer algorithms that use objective measures from the network.

    b. Latency is the time it takes for a voice packet to traverse the network.

    c. Jitter is caused by variable arrival times of voice packets. A buffer, or delay, is created to wait for packets that arrive out of sequence.

    d. Lost packets are voice packets that do not reach the endpoints to be processed for the voice conversation. A single lost packet is usually not noticeable, but packet loss frequently occurs in bursts where many packets are lost in a group.

    e. It is commonly accepted that it must take no more than 150 milliseconds for a voice signal to pass from the caller’s mouth to the callee’s ear to realize acceptable voice quality.

3. Increasing bandwidth can help to improve voice quality in some regards, but is usually not the best method to address poor quality.

4. Echo is frequently encountered when implementing IPT. It iscreated when the receiver's telephony equipment amplifies and returns parts of the original signal back to the sender. It negatively impacts the conversation when the delay is greater than 25 milliseconds. It can be reduced by properly configuring echo cancellers that are equipped with most IPT devices

5. Quality of Service (QoS) mechanisms must be used to maintain good call quality on a converged network. QoS mechanisms give time-sensitive packets like IPT traffic priority over other traffic, like email, to increase the probability that voice packets will arrive quickly enough to achieve good call quality.

## E. RESILIENCE

**1.** The PSTN provides "five nines" of availability (99.999%), meaning that the telephone network is done less than six minutes a year. IPT-based networks require a variety of backups to approach this level of service, including redundant: power, memory, systems, applications, network components, and out-of-band communications (e.g., PSTN line).

**2.** PSTN lines provide power to telephone components, even in times where local power is down. IPT-based networks require extra consideration for providing local power to equipment during power outages.

## F. POWER AND REACH

1. Many phones are located in places where there is no need for computers, so there is not any power or network wiring in place. Sometimes these points are extended using wireless devices. Units must be prepared to provide for these areas when deploying IPT, and understand the potential reductions in voice quality to create solutions.

## G. NETWORK MANAGEMENT

1. IPT-based networks are not managed in the same manner as the data network. Data network personnel and telephony personnel must work together and learn new skills to properly manage the IPT network. The network will require constant attention and tuning to assure quality and availability. The support of the network should be facilitated by network management tools that are specifically attuned to the needs of IPT.

## H. PLATFORM INDEPENDENCE/SUPPORT OF LEGACY SERVICES

1. A successful IPT implementation will facilitate interoperability among telephony components and be flexible to adapt to changes in the technology.

2. Few telephony networks are solely devoted to IPT technology, but rather integrate a variety of networks to provide a competitive telephony solution. It requires careful planning to connect the IPT network to other networks, like the PSTN or an ISDN, and to connect a variety of equipment from multiple vendors.

3. Successful implementations avoid propriety equipment and protocols, and strive for standards that bring a diverse set of elements together to form a reliable telephone system.

## I. SCALABILITY

1. An IPT-based network, its equipment and protocols, must be flexible enough to grow and change with the organization.

2. Most IPT implementations do not completely replace existing telephony solutions; rather, they are incrementally deployed to achieve better value.

## J. FEATURES

1. The primary business advantage that is beginning to emerge from IPT is the diverse set of features that it promises to provide. To maximize the benefit of an IPT implementation, Coast Guard organizations must create IPT solutions that enable feature sets that optimize current operational practices and understand how those features differ from current PSTN offerings.

## K. USER MOBILITY

1. One of the advantages of IPT is the mobility that it provides to employees. This mobility can be manifest in a user’s ability to quickly change desks, change phones, or even work out of the office at home or on the road. These benefits require additional security and QoS measures to appropriately implement.

## L. EMERGENCY SERVICES

1. Emergency 911 location services are a standard part of the PSTN that many people take for granted. These services require special measures (especially due to increased mobility) to ensure the same level of reliability that the PSTN already provides. Coast Guard units must ensure appropriate systems are in place to protect human resources.

# CHAPTER 3 IPT IMPLEMENTATION PRACTICES

## A. PURPOSE

1. The following section enumerates and explains a variety of practices that organizations are using to successfully implement IPT and address the issues discussed in the previous section. The methods described below are not necessarily conducted in the order listed. Some may be performed simultaneously, while other groups of processes may require multiple iterations to design the right IPT solution. The practices discussed should be adapted to meet the needs of a Coast Guard organization within the context of its environment.

2. The implementation practice considerations are separated into nine elements: (1) Form an Implementation Team, (2) Understand Current Telephony Requirements, (3) Understand the Data Network Infrastructure, (4) Upgrade the Data Network, (5) Develop the Business Case & Acquire, (6) Create an Implementation Plan, (7) Deployment, (8) Network Management & Maintenance, and (9) Manage Change.

## B. SECURITY

1. Security must be considered throughout the implementation process, but will not be addressed in detail in this Appendix. IPT-based network security issues are addressed in Appendix A and other Coast Guard Security Policy.

## C. COAST GUARD POLICY

1. COMDTINST 5230.66, The Coast Guard Command, Control, Communications, Computers, and Information Technology (C4&IT) Systems Development Life Cycle (SDLC) Policy has a sequence of seven phases that are used to produce, operate, and support C4&IT. They include: (1) Conceptual Planning, (2) Planning and Requirements Definition, (3) Design, (4) Development and Testing, (5) Implementation, (6) Operations and Maintenance, and (7) Disposition (or System Retirement). The recommendations provided in this document differ in the following aspects:

    a. The recommendations that follow are specific to IPT-based networks and components.

    b. The SDLC policy addresses similar issues, but appears to do so with a waterfall approach. That is, each step of the life cycle is almost fully completed before moving on to the next step. The recommendations that follow recognize that successful IPT implementations are often incremental, and the phases of development often overlap or require several iterations to produce the right solution.

    c. The recommendations that follow do not address the disposition of IPT-based networks.

d. The recommendations that follow specifically addresses change management, in regards to managing personnel and business processes as the organizational element transitions from traditional telephony and data networks to a converged network.

## D. FORM AN IMPLEMENTATION TEAM

1. Since IPT brings together the data network and the telephone network, personnel with training and experience from both backgrounds are required to understand the new system. Form a team that taps the resources of employees with varying specialties (e.g., telephony specialist, network manager, security professional, finance, legal, educational, etc.) so that all issues may be addressed.

2. Team members must receive the training and develop the experience necessary to interface ideas and processes. Collaboration must be encouraged to exchange and fuse information.

3. The project team must be given adequate sources of power (e.g., budget, resources, management support, etc.) to plan and implement the new IPT system.

4. The IPT implementation team may be supported by outside personnel, called system integrators, who are brought in to help design an IPT solution. Outsourcing pieces of the implementation has the advantage of providing in-depth knowledge and experience about IPT. This know-how usually comes more quickly and at a lower cost than training internal IPT experts.

5. When selecting system integrators, review and weigh the integrators' level of quality, expertise, capability, integrity and cost. The contract with the system integrator should include service-level agreements, training and support so that the system is properly maintained when the system integrator leaves.

## E. UNDERSTAND CURRENT TELEPHONY REQUIREMENTS

1. Use Call Detail Records (e.g., monthly itemized bill) to track statistics of interest that will help to understand current telephony usage. These statistics include: number of calls, number of users with distinct phone numbers, duration of calls, number of concurrent calls, source and destination of calls (within site, within business, external, international versus domestic), and call volumes.

   a. Call volume profiles are especially important for determining network capacity. Call volume peaks and averages should be discovered with an understanding of when peaks occur, for how long, and if they cause (a percentage of) blocked calls.

2. Review telephony costs and carrier contracts. Identifying these costs helps to justify the IPT implementation, but may also point out potential areas of increased costs. For instance, a unit that deploys IPT may reduce the number of calls on the PSTN, but actually cause an increase in telephony costs. This can happen when

the reduced PSTN call volume falls below a threshold where "bulk" rates are applied. Even though there are fewer calls, those calls become more expensive and may actually drive up costs.

3. Review telephony system maintenance costs, including equipment and personnel.

4. Determine the costs of Moves, Adds, and Changes (MACs). An example of a MAC happens when a person moves to a new office with his/her phone and number. The administrative process is often expensive and slow due to limitations of PSTN design.

5. Determine what level of availability your current telephone system actually provides. Is it 99.999% or actually something less than that?

6. Determine what functions and features the current system provides to users. Find out which ones they actually use, and prioritize them. Solicit ideas for new features. Manage user expectations.

   a. Examples of telephony requirements include: voice mail, conferencing, customer relationship management tools (a.k.a. phone trees), simple phone interfaces, simple dialing plans (how many extra numbers does the user need to dial to get an outside line balanced with how few to dial internal extensions), Caller ID, Call waiting, number of lines, voice quality, reliability, E911, accessibility, mobility, fax, modem, etc.

## F. UNDERSTAND THE DATA NETWORK INFRASTRUCTURE

1. IPT cannot be placed on top of the data network like any other application. Data network adjustments and more stringent monitoring are required to ensure acceptable security and call quality. Implementation failures and difficulties are often attributed to insufficient network preparation.

2. Conduct a data network audit to identify the current characteristics of the data network so that adjustments can be made to support IPT. This type of evaluation must be performed at three levels as appropriate to the implementation: (1) over the local area network, (2) over the enterprise wide area network, and (3) over the Internet (although the ability to make changes will be limited). The audit may be conducted by focusing on the four areas provided: Configuration Assessment, Utilization Assessment, Call-Quality Assessment, and Bandwidth Modeling.

   a. **Configuration Assessment**: The purpose of this assessment is to examine network equipment to determine what must be upgraded to handle IPT. First, all network equipment must be identified and inventoried. The equipment characteristics that should be checked include:

      (1) Operating system version,

      (2) Memory,

(3) QoS mechanisms,

(4) VLANs (data, voice, and wireless should be separate & hubs should be removed),

(5) Interface speeds, and

(6) Power supplied to the phone.

Then each piece of equipment must be compared to a set of criteria to determine if it will support IPT: traffic, functionality, capacity, reliability and call-quality. For example, a configuration assessment might reveal that a network router has an interface speed of 100 megabits per second (Mbps). Based on peak call volumes, the speed will not be able to handle all calls without degraded call quality or dropped calls. The router must be upgraded (e.g., 1000 Mbps) to support the new IPT-based network.

b. **Utilization Assessment**: The purpose of this assessment is to identify to what degree network devices and links are being utilized. Average values, peak values, and times of high utilization are important metrics to observe. Utilization rates that approach 100% suggest problem areas for IPT implementation, which must be managed or corrected via equipment upgrades. The following dimensions should be measured to ensure the support of IPT: traffic, functionality, capacity, reliability and call-quality:

(1) CPU utilization (device's workload),

(2) Memory utilization (e.g., size of jitter buffer),

(3) Backplane utilization (amount of traffic moving through switches),

(4) Dropped packets (occur at bottlenecks),

(5) Buffer errors (usually indicates inadequate memory),

(6) Interface errors (usually indicate problems with physical transport medium), and

(7) Bandwidth utilization (the percentage of bandwidth being used). Bandwidth utilization is a good indicator of network capacity and should always be closely monitored, particularly on wide area network links where delays are more likely.

c. **Call-Quality Assessment**: The purpose of this assessment is to determine how well the network would support good call quality by simulating IPT traffic and measuring the flow of information for delay, jitter and packet loss. These measurements are used to estimate a mean opinion score to determine

call quality. The following characteristics of IPT equipment and packets will affect the flow of information:

(1) The type of codec used (the compression algorithms and data rates it uses, and the packet size it produces).

(2) Voice packet sizes (smaller packets move more quickly but have more overhead).

(3) The use of Voice Activity Detection (VAD) (smaller packets of information are sent when there is silence on the line between phrases).

(4) The size of jitter buffers.

(5) QoS mechanisms.

The simulation allows experimentation among changes in network characteristics and is usually conducted on selected portions of the network that mostly represent the entire IPT network. From this assessment, predictions can be made about the feasibility of good call quality in an IPT implementation. It is also useful for identifying potential risks and weak points in the network prior to deployment, allowing for equipment upgrades or network configurations that will enhance call quality.

d. **Bandwidth Modeling**: The purpose of this assessment is to make predictions about the actual performance (not necessarily call quality) of the current network with the load of IPT traffic. This process is very similar to the call quality assessment described above, but is more complex and requires many mathematical calculations to complete. If possible, conduct bandwidth modeling on critical network links first and expand as resources permit. Bandwidth modeling allows the IPT design team to determine how well the capacity of the network handles the additional traffic introduced by IPT, based on changes in call volumes, codecs, bandwidth, packet sizes, QoS, and voice suppression mechanisms.

## G. UPDATE THE DATA NETWORK

1. After successfully auditing the data network, many changes are required to adequately support IPT. Network changes usually focus on call quality improvements or replacing equipment to meet other requirements like security or redundancy.

2. Increased call quality can be achieved by cleaning up network traffic, increasing bandwidth, upgrading equipment, changing the network design, and implementing or tuning QoS mechanisms.

a. **Network Traffic**: Approximately 20%-50% of network traffic is considered unnecessary, supporting unneeded services that are operating by default,

usually without anyone's knowledge. Use a network protocol analyzer (e.g., Ethereal, EtherPeek) to identify these. Turning them off will increase bandwidth, and reduce the load on processors and memory.

b. **Bandwidth**: There are several methods available that help to conserve bandwidth, some of which include:

(1) RTP header compression (cRTP): cRTP compresses RTP headers to reduce bandwidth consumption, but comes at the expense of increased handling delay.

(2) VAD: VAD reduces bandwidth consumption by sending smaller packets during silence, but can reduce voice quality.

(3) RTP multiplexing: RTP multiplexing sends several voice conversations in the same packet to cut out bandwidth that is consumed by headers, but can add to delay and cause greater impact when packets are lost.

(4) Call admission control. Call admission control is used to limit the number of concurrent IPT calls on the network, routing extra calls to the PSTN.

The benefits and disadvantages of each of these methods must be balanced to meet the requirements of the network configuration. If these mechanisms aren't sufficient to free up adequate bandwidth it may be appropriate to pay for more; however, it is important to understand the network in order to increase the bandwidth in the bottlenecks where it is needed the most.

c. **Equipment**: Common equipment upgrades to improve voice quality include:

(1) Replacing hubs with switches,

(2) Upgrading to more modern switches and routers that process information more quickly,

(3) Increasing Router memory, and

(4) Preferring hardware-based firewalls to software-based equipment.

These equipment upgrades help increase the processing speed of the network, enabling better call quality.

d. **Network Design**: Re-engineer the network to improve call quality:

(1) Examine traffic flow to determine what kinds of routes are used and how many hops are required to get from one endpoint to another. Direct, shorter routes and fewer hops will help to reduce propagation and handling delays.

(2) Locate bottlenecks and points of congestion. Work to eliminate them, route around them, or give precedence to IPT traffic.

(3) Push processing work out to the endpoints to facilitate the movement of packets through the core of the network. This, however, requires more processing power at the edges of the network.

e. **QoS Mechanisms**: QoS mechanisms give priority to time-sensitive applications like IPT. They help to maintain good call quality during occasional periods of congestion.

3. When updating network equipment, make changes methodically.

   a. Prioritize: determine which changes are the most cost effective and most important.

   b. Incremental adjustments: start with the highest priorities and make small changes. Those that try to make too many modifications at once find that it is too difficult to identify new problems created by the change.

   c. Test: conduct assessments to ensure that changes have the desired effect.

   d. Repeat: The incremental, iterative approach makes it easy to adjust priorities and determine when network improvements have reached an acceptable level to meet IPT network performance criteria.

## H. DEVELOP THE BUSINESS CASE & ACQUIRE

1. Justifying the installation of an IPT-based network occurs prior to and throughout the implementation process. The planning and preparation phases discussed to this point help to strengthen a case to deploy IPT (or not to deploy it) by determining requirements and by assessing the condition of the data network. These considerations must be weighed with an analysis of the costs required to go forward with a large scale implementation. A project team that is able to demonstrate measurable benefits and the viability of IPT early and continuously will get internal commitment and budgetary support that will sustain the duration of the implementation.

2. IPT-based networks are rarely deployed by completely replacing old PSTN equipment with new IPT gear. The benefits of IPT are usually realized through incremental upgrades that take advantage of the features of both IPT and the PSTN. The following scenarios are examples of upgrades that promise large returns from minor investments for most organizations.

   a. **New Sites**: Expanding to a new site allows a unit to build new telephony service from the ground up without having to worry about upgrading an old network. With proper planning, the new office can provide dependable IPT service with room for future growth.

b. **Data Network Upgrades**: If the data network is already in need of an improvement, it is appropriate to piggy-back IPT requirements in the planning process.

c. **Excess Capacity**: Bandwidth and processing power have become very inexpensive. Consider IPT if you have recently upgraded the data network with increased speed and capacity.

d. **Expiring Service Contracts**: The possibility of shifting some telephony expenses to the data network may be convenient when leases expire, but also adds leverage to bargaining power when renegotiating.

e. **Voice Network Upgrades**: If the current voice network is not meeting operational requirements it is a good opportunity to incrementally add and test new IPT services that will eventually lead to larger deployments.

f. **Remote Users**: IPT can provide telephone support to telecommuters with high speed connections.

3. **Equipment**: To avoid additional costs and network difficulties, all IPT equipment should be non-proprietary and interoperable. The use of proprietary equipment often prevents equipment (from different vendors) from communicating correctly and can lock you into a position where you must continue to rely on one vendor for service. This lack of flexibility puts you at the mercy of the vendor, creating the potential for inflated costs or system failure should the vendor company collapse or fail to keep up with operational needs. Support vendors that produce interoperable, open architecture systems. This facilitates the development of equipment that easily communicates between different types of networks, protocols, and vendor equipment. Until common IPT standards are realized, prefer equipment that provides the most interoperability (e.g., IPT equipment that supports both SIP and H.323).

4. **Services**: A Service Level Agreement (SLA) is an agreement between the user and a vendor that defines what services will be provided, at what cost, how they will be measured, and how deficiencies will be addressed. When working with service vendors, agree on measurable SLAs that are easy to enforce (because they include specific actions when guarantees aren't fulfilled).

5. **Outsourcing**: All of the practices discussed in this document could potentially be outsourced to another company. Outsourcing is the practice of hiring another company to handle an internal business function, usually because we believe that someone else can do it better at a lower cost. Outsourcing options can range from an entire IPT deployment to portions of it, like the data network assessment or network upgrades. Hiring a system integrator is also a form of outsourcing. Almost anything can be outsourced; however, as the level of outsourcing and reliance on the vendor increases, the level of internal control of the IPT network decreases.

a. When outsourcing any of the IPT implementation or IPT services, work to create a relationship with the provider that will lead to long term success of the IPT deployment. This can be done by avoiding the following six mistakes:

(1) Not clearly defining the desired results and how they'll be measured,

(2) Not talking to a provider's current and former clients,

(3) Failing to consider the long-term relationship dynamics,

(4) Signing a standardized, multiyear contract,

(5) Not planning up front for how the relationships might end, and

(6) Treating the provider as an outsider.

6. Acquire all IPT equipment in accordance with appropriate Coast Guard Policy:

a. *Coast Guard Command, Control, Communications, Computers, and Information Technology (C4&IT) Investment Management Policy*, COMDTINST 5230.71.

b. *Coast Guard Acquisition Procedures (CGAP)*, COMDTINST M4200.19 (series).

c. *U.S. Coast Guard Logistics Handbook*, COMDTINST M4000.2.

## I. CREATE AN IMPLEMENTATION PLAN

1. An effective method of implementing IPT is to make incremental adjustments. An IPT implementation plan is designed with this in mind and identifies distinct breaks in the process where effectiveness can be measured. A proven method to start the process is to conduct a pilot deployment. This gives the IPT project team the opportunity to gain experience with the technology before diving into a full deployment. The pilot program helps the project team to truly understand how the IPT-based network will function in the organization and enables them to create an implementation plan that addresses the highest priorities first.

2. **Pilot Deployment (Test Bed)**: A pilot program is a small implementation of IPT intended to be a learning opportunity that prepares for a larger implementation; however, it also helps to define a business case for IPT and helps to select the best equipment and services for a full deployment.

a. The best places to perform the pilot is in a situation where:

(1) Return on investment is high (see section H.2 of this chapter),

(2) Potential for disruption is minimal,

(3) User cooperation and feedback is high.

b. To get the most out of the test bed, the project team should learn as much as they can about the behavior of the system:

(1) Experiment with different equipment, configurations, traffic volumes, protocols, QoS mechanisms, and security mechanisms.

(2) Understand how equipment from different vendors interoperates.

(3) Understand how to recognize, isolate, and repair network problems.

(4) Supported experimentation with training and with strong working relationships with potential vendors.

(5) Become familiar with the maintenance and long term management of the system to ensure success when vendor support fades.

c. The more thorough the pilot program, the more prepared the project team will be for a large scale deployment of IPT.

## J. DEPLOYMENT

1. Once a pilot program has been conducted and an implementation plan is developed, the project team will be prepared to move into full deployment. The project team should begin to make adjustments to the network incrementally and be prepared for adjustments. Changes in the plan will effectively be recognized by building feedback loops into the process and by monitoring measurements that demonstrate system effectiveness. Examples of tests that might be used to check each phase of the implementation is provided below. A systematic and continuous assessment of the implementation creates a smooth transition to a valuable IPT-based network.

a. *Operation and Function Test*: Does all the end-user equipment work properly and provide all promised features?

b. *Ease of Use Test*: Is the system easy for all users to use? Is the system easy for the IT staff to maintain?

c. *Network Application Performance Test*: Is there good call quality?

d. *Transaction-oriented Application Performance Test*: Are critical applications on the network still operating normally after the change? This requires the project team to take measurements prior to the change.

e. *Settings Test*: Do equipment and applications still perform as expected after changing IPT configurations?

f. *Stress Test*: Does the network provide good call quality to the predicted level of call volume? Does it transfer calls to the PSTN when the limit is reached?

g. *Extraneous Traffic Test*: Is the system doing anything you don't expect or understand? A network protocol analyzer may help to determine this.

h. *Problem Reporting Test*: Does the IPT management system operate correctly? Create faults in the system and see if the management system responds accordingly.

## K. NETWORK MANAGEMENT & MAINTENANCE

1. Once the IPT-based network has been deployed, it requires constant attention to maintain high levels of reliability, call quality, and system security. An effective IPT management system will meet the future needs of a growing network while addressing four areas of concern: Operations, Availability, Call Quality, and Accounting. Security is an important piece of each area and must be consistently addressed to assure the well-being of the network.

2. **Managing Operations**: Use configuration management, event management, and fault management to identify and address problems proactively to prevent significant system failures.

   a. **Configuration Management**: A configuration is the hardware and software arrangements that define a computer or telecommunications system and thus determine what the system will do and how well it will do it. To manage the IPT system configuration, the IT staff must:

   (1) **U**nderstand the current configuration,

   (2) Test and monitor all changes to the system configuration,

   (3) Closely track all changes, and

   (4) Limit and control who is authorized to make changes.

   An awareness of the current system configuration is achieved through the use of readable and understandable files, reports, and diagrams. The network management team must understand what physical components make up the network, they should know equipment specifics, and recognize how the components are linked together. This can be accomplished through the use of network topology diagrams and up-to-date inventories. Topology diagrams provide a good high-level understanding of how the network is connected. Inventories provide more specific information (e.g., Name, location, IP and MAC addresses, function of the device, vendor, model, serial number, operating system version, available memory, processing speed, etc.) to better understand each components function in the network. There are also software tools available to help identify and track this information. Configuration files

should be protected to ensure the current configuration is accurate. This is accomplished by limited access to authorized individuals, by backing up configuration files frequently, installing security mechanisms, and by closely monitoring access to the files in order to recognize potential damage.

b. Perform configuration management in accordance with appropriate Coast Guard Policy:

(1) *Coast Guard Command, Control, Communications, Computers, and Information Technology (C4&IT) Configuration Management (CM) Policy*, COMDTINST 5230.69.

(2) *Standard Workstation III Configuration Management Policy*, COMDTINST 5200.16.

c. **Event Management**: Operating systems have the ability to track and log a variety of system events (e.g., opening, reading, modifying, and closing documents; when an application starts and stops; system errors). When system performance suffers, failures occur, or when the network has been attacked it is usually possible to recognize signs of the cause through system logs.

(1) Prioritize system events. It is infeasible to keep track of them all, so track and log only those events that can effectively acted on.

(2) Determine what kind of system response is required to address suspicious activity, which might include alerting the IT staff or executing corrective action without immediate human intervention.

(3) Use software applications that help to track system events, consolidate logs, and help to recognize irregular activity.

d. **Fault Management**: The IPT system management team must be able to locate and correct system problems quickly as a part of day-to-day operations to prevent significant downtime.

(1) The complexity of the network often makes it difficult to isolate problems. A team can do several things to locate problems more quickly:

(1) Look in places where recent changes were made,

(2) Look in places where previous failures occurred, and

(3) Look in places where monitoring indicates a trend of increasing trouble.

(4) Track the logical path between two endpoints where the problem occurs.

(2) Track all problems, whether solved or still unidentified, with an explanation of symptoms, expected time and cost to repair, solutions, and a priority. This will help the management team to address the most important problems first and create a repository of information that will enable faster resolution in later cases.

(3) Create a plan to handle significant events, like a network failure or severe attack on security (e.g., DDoS), so that the problem can be addressed efficiently (i.e., decreasing the likelihood of long hours that can cause more failures due to human fatigue and limitations) before significantly impacting operations.

3. **Maintaining High Availability**: Reduce network downtime through prevention, detection, and reaction. Focus efforts on IPT servers and managing applications.

    a. *Prevention*: The best approach is to prevent failures by actively responding to small indications of problems before they get out of control.

    b. *Detection*: When prevention is not successful, the IT team must be able to quickly isolate the problem so that it can be repaired.

    c. *Reaction*: Once detected, the team must act quickly to provide a short term solution and follow up with a permanent fix and preventions for similar failures.

    d. *IPT servers*: IPT servers provide the most critical portions of the network. Harden servers to maintain a strong security posture and monitor them continously with a focus on the hardware, applications, and traffic.

    e. *Manage Applications*: System software is complex and often acts unexpectedly, especially when interacting with other applications. Applications can often consume resources quickly or waste processing capability on unnecessary operations. Setting limits and closely monitoring these systems assists in achieving better levels of availability.

4. **Maintaining Consistent Call Quality**: On initial deployment, the IPT-based network should provide satisfactory call quality. However, as the network grows and changes, call quality is likely to become an issue.

    a. *Measure and track current call quality*: Toll quality is measured at an MOS of 4.0 or greater, while quality becomes unacceptable at levels lower than 3.6. Software is available to continuously monitor network traffic and determine an estimate of the MOS. Monitoring should occur throughout the network and trigger a response (e.g. alert staff or divert calls) when quality falls below established standards.

   b. *Monitor network performance*: The network metrics for IPT that should be examined most closely are delay, jitter, and lost packets. Responding to fluctuations in these measurements help to maintain call quality.

   c. *Enforce SLAs*: Delay, jitter, and lost packet measurements are typically used to establish service level agreements with service providers. Track them and hold vendors accountable to encourage consistent quality.

   d. *Tune QoS mechanisms*: QoS mechanisms must be managed to ensure that they are configured correctly and work correctly. The mechanisms can be complex, but can be managed with policy-based network management. A policy server monitors how traffic is handled and automatically generates and distributes configuration instructions that help components to apply QoS settings in accordance with policy.

   e. *Plan for future growth*: Prepare for future growth by tracking how the network responds when new users are added. Understanding these trends assists in determining how to incrementally install or upgrade components in response to increasing call demands.

5. **Accounting**: Call detail records (CDRs) are used to keep track of the details of completed calls, containing information like the call source, destination, time, duration, delay, and jitter.

   a. Use the information in CDRs to monitor and troubleshoot the network.

   b. Use the information in CDRs to determine who pays for what IPT service.

   c. Closely track and monitor CDRS to ensure accurate billing and to help identify potential problems in the network.

   d. Protect CDRs, they usually contain personal or private information that is protected by law.

6. Failure to successfully monitor and upkeep the network can create substantial losses due to the costs of replacing damaged equipment, time lost by the IT staff, lowered employee productivity, and the loss of customer or public trust. Good IPT network management will come at an increased cost of human and physical resources, but is necessary to balance the risks of network failures that hamper operations.

## L. MANAGE CHANGE

1. The final capabilities that are used in successful deployments are: the ability to manage the expectations of the people who will use the new system and the ability to adjust operational processes to utilize new technology.

2. Employees can be a great hindrance to any significant change in an organization, including the introduction of an IPT-based network. They have a variety of reasons, whether it is because they are comfortable with the old way of doing business or because they believe they will lose power or because of any other reason. Harness the drive of those who are excited to implement the change and manage those who are likely to resist.

3. The introduction of IPT will not only change the equipment in the business, but is likely to have an effect on how business is done in order to take full advantage of the opportunity. An implementation of IPT must include a reevaluation of operational processes that utilize telephony resources.

4. There are many methodologies that have been created to manage this type of change in the organization, and many of them could be applied to an IPT implementation. An example of a change management methodology is discussed below to demonstrate the use of techniques that might smooth out the transition to IPT. A framework for business transformation, which may be applied to IPT implementations, is explained by Joseph Kotter in the article, "Leading Change: Why Transformation Efforts Fail." It consists of eight steps that are discussed below.

    a. **Establishing a Sense of Urgency**: The urgency that must be conveyed for an IPT implementation is the opportunity to realize great benefits from a converged network. That urgency may soon be created by the need to keep up with other governments or agencies that have already taken advantages of IPT-based networks. The level of urgency is established by the effectiveness of the business case made to stakeholders of an IPT system.

    b. **Forming a Powerful Guiding Coalition**: The IPT implementation project team will lead the development, but can only do it effectively with the support (in the form of budget and authority) of upper management. They can also drive positive change with the support of enthusiastic employees that have an interest in the end product.

    c. **Creating a Vision**: The vision is supported by a strong business case and a well-planned implementation plan, which includes plans for development beyond the initial deployment and changes in operational and administrative processes.

    d. **Communicating a Vision**: All stakeholders, down to individual users, must have an understanding of the changes that will take place to convert to IPT technology and resultant business practices. This is accomplished through training and continuous communication that includes feedback between both implementers, stakeholders, and users.

    e. **Empowering Others to Act on the Vision**: This is accomplished by getting full support from individuals who have the authority and budget to make

changes. Enthusiast stakeholders will lose faith if not given the power to implement the IPT system the right way.

f. **Planning for and Creating Short-Term Wins**: Small deployments and pilot projects, which take advantage of great returns from small changes, will help to achieve buy-in from stakeholders. It is also an early indication of problems or resistance if a project team is unable to get user acceptance or realize business improvements on small changes. Successes, however, should be recognized to encourage further growth, acceptance, and positive business change.

g. **Consolidating Improvements and Producing Still More Change**: The incremental approach to implementing IPT-based networks provides an excellent method to encourage positive change. The process produces gradual change in stages and confirms success through effective measures of performance. Not only must the technical aspects of the change be measured as described, but the project team must also monitor the effect those changes have on business processes. Incremental successes build upon each other to create more positive change and acceptance in the future.

h. **Institutionalizing New Approaches**: Finally, the implementation will be a success when stakeholders adjust to and accept new business processes created by the change in technology. Be wary of those who continue to reminisce about the way things used to be, and reward those who embrace the opportunity to improve operational capability through the use of IPT.

THIS PAGE INTENTIONALLY LEFT BLANK

# INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Professor Dan C. Boger
   Naval Postgraduate School
   Monterey, California

4. R. Scott Coté
   Naval Postgraduate School
   Monterey, California

5. CDR Kip Whiteman
   USCG Headquarters Support Command
   Washington, D.C.

6. Tom Estes
   USCG Headquarters Support Command
   Washington, D.C.

7. CWO Lewis Darley
   USCG Headquarters Support Command
   Washington, D.C.

8. CDR Tom Pedagno
   USCG COMMANDANT(CG-621)
   Washington, D.C.

9. Tom Clark
   Telecommunications and Information Systems Command
   Alexandria, Virginia

10. LT Mark Patton
    Cottage Grove, Oregon